09/807824

PCT/JP00/05543

18.08.00

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９９年１２月２１日

出 願 番 号
Application Number: 平成１１年特許願第３６３２６６号

出 願 人
Applicant (s): ソニー株式会社

PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

２０００年 ６月２９日

特 許 庁 長 官
Commissioner,
Patent Office 近 藤 隆 彦

出証番号 出証特２０００－３０５００８５

【書類名】　特許願

【整理番号】　9900664607

【提出日】　平成11年12月21日

【あて先】　特許庁長官殿

【国際特許分類】　G11B　7/00

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　浅野　智之

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　大澤　義知

【特許出願人】

【識別番号】　000002185

【氏名又は名称】　ソニー株式会社

【代表者】　出井　伸之

【代理人】

【識別番号】　100067736

【弁理士】

【氏名又は名称】　小池　晃

【選任した代理人】

【識別番号】　100086335

【弁理士】

【氏名又は名称】　田村　榮一

【選任した代理人】

【識別番号】　100096677

【弁理士】

【氏名又は名称】　伊賀　誠司

【先の出願に基づく優先権主張】

【出願番号】　平成11年特許願第234371号

【出願日】　平成11年 8月20日

【手数料の表示】

【予納台帳番号】　019530

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9707387

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報記録／再生システム、情報記録／再生装置及び方法、情報記録媒体、記録媒体製造装置及び方法

【特許請求の範囲】

【請求項１】　セキュリティモジュールを有する情報記録媒体と、上記セキュリティモジュールが管理する暗号鍵によって暗号化されたデータを上記情報記録媒体に記録、あるいは、上記セキュリティモジュールが管理する暗号鍵によって暗号化されたデータを上記情報記録媒体から再生する情報記録／再生装置とを備え、

情報記録時、又は情報再生時に上記情報記録／再生装置とセキュリティモジュールとが公開鍵暗号技術を用いた相互認証プロトコルを実行することを特徴とする情報記録／再生システム。

【請求項２】　上記相互認証プロトコルの実行時に、上記記録／再生装置とセキュリティモジュールが、互いに、他方の識別情報がリボケーションリストに掲載されていないことを確認することを特徴とする請求項１記載の情報記録／再生システム。

【請求項３】　上記セキュリティモジュールと上記情報記録／再生装置の何れか一方若しくは両方がリボケーションリストを保持する保持手段を備えるか否かに応じた相互認証プロトコルを使用することを特徴とする請求項１記載の情報記録／再生システム。

【請求項４】　上記相互認証プロトコルの実行時に、上記記録／再生装置とセキュリティモジュールが、互いに、自分が所有するリボケーションリストのバージョンナンバーを教え合い、新しいリボケーションリストを持つものがそれを他方に送り、古いリボケーションリストを持つものは送られた新しいリボケーションリストを用いて自分のリボケーションリストを置き換えることを特徴とする請求項１記載の情報記録／再生システム。

【請求項５】　上記記録／再生装置とセキュリティモジュールの両者は、共に上記新しいリボケーションリストを用いて、上記相互認証プロトコルを実行することを特徴とする請求項４記載の情報記録／再生システム。

【請求項６】　上記相互認証プロトコルの実行時に、上記記録／再生装置とセキュリティモジュールが、互いに、他方の識別情報がレジストレーションリストに登録されていることを確認することを特徴とする請求項１記載の情報記録／再生システム。

【請求項７】　上記セキュリティモジュールと上記情報記録／再生装置の何れか一方若しくは両方がレジストレーションリストを保持する保持手段を備えるか否かに応じた相互認証プロトコルを使用することを特徴とする請求項１記載の情報記録／再生システム。

【請求項８】　上記相互認証プロトコルの実行時に、上記記録／再生装置とセキュリティモジュールが、互いに、自分が所有するレジストレーションリストのバージョンナンバーを教え合い、新しいレジストレーションリストを持つものがそれを他方に送り、古いレジストレーションリストを持つものは送られた新しいレジストレーションリストを用いて自分のレジストレーションリストを置き換えることを特徴とする請求項１記載の情報記録／再生システム。

【請求項９】　上記記録／再生装置とセキュリティモジュールの両者は、共に上記新しいレジストレーションリストを用いて、上記相互認証プロトコルを実行することを特徴とする請求項８記載の情報記録／再生システム。

【請求項１０】　上記相互認証プロトコルの実行時に、上記記録／再生装置とセキュリティモジュールが、互いに、他方の識別情報がリボケーションリストに掲載されていないこと、及び／又は、レジストレーションリストに登録されていることを確認することを特徴とする請求項１記載の情報記録／再生システム。

【請求項１１】　上記セキュリティモジュールと上記情報記録／再生装置の何れか一方若しくは両方がリボケーションリスト及びレジストレーションリストを保持する保持手段を備えるか否かに応じた相互認証プロトコルを使用することを特徴とする請求項１記載の情報記録／再生システム。

【請求項１２】　上記相互認証プロトコルの実行時に、上記記録／再生装置とセキュリティモジュールが、互いに、自分が所有するリボケーションリスト及びレジストレーションリストのバージョンナンバーを教え合い、新しいリボケーションリスト及びレジストレーションリストを持つものがそれを他方に送り、古い

リボケーションリスト及びレジストレーションリストを持つものは送られた新しいリボケーションリスト及びレジストレーションリストを用いて自分のリボケーションリスト及びレジストレーションリストを置き換えることを特徴とする請求項１記載の情報記録／再生システム。

【請求項１３】　上記記録／再生装置とセキュリティモジュールの両者は、共に上記新しいボケーションリスト及び／又はレジストレーションリストを用いて、上記相互認証プロトコルを実行することを特徴とする請求項１２記載の情報記録／再生システム。

【請求項１４】　上記相互認証プロトコルの実行時に、上記記録／再生装置とセキュリティモジュールが、リボケーションリストとレジストレーションリストのうち何れか一方を選択的に使用することを特徴とする請求項１記載の情報記録／再生システム。

【請求項１５】　データの記録時又は再生時に、上記情報記録／再生装置とセキュリティモジュールが公開鍵暗号を用いて鍵共有プロトコルを実行し、共有された鍵を用いてデータを暗号化する暗号鍵を一方が暗号化して他方に送ることを特徴とする請求項１記載の情報記録／再生システム。

【請求項１６】　データの記録時又は再生時に、上記情報記録／再生装置とセキュリティモジュールが公開鍵暗号を用いて鍵共有プロトコルを実行し、共有された鍵を用いてデータを一方が暗号化して他方に送ることを特徴とする請求項１記載の情報記録／再生システム。

【請求項１７】　データを格納する情報記録媒体への書き込み、読み出しのアクセスは、上記セキュリティモジュールを介して行われることを特徴とする請求項１記載の情報記録／再生システム。

【請求項１８】　データの記録時に、上記情報記録／再生装置とセキュリティモジュールが公開鍵暗号を用いて鍵共有プロトコルを実行し、共有された鍵を用いて上記情報記録／再生装置がデータを暗号化してセキュリティモジュールに送り、上記セキュリティモジュールは、共有された鍵を用いてこれを復号して平文データを得た後に、暗号鍵を用いてデータを暗号化して情報記録媒体に格納することを特徴とする請求項１７記載の情報記録／再生システム。

【請求項１９】　データの再生時に、上記セキュリティモジュールが暗号化されて情報記録媒体に格納されているデータを読み出し、暗号鍵を用いてこれを復号して平文データを得た後、上記情報記録／再生装置とセキュリティモジュールが鍵共有プロトコルを実行した結果共有された鍵を用いてデータを上記セキュリティモジュールが暗号化して情報記録／再生装置に送ることを特徴とする請求項１７記載の情報記録／再生システム。

【請求項２０】　データの記録時及び再生時に、情報記録／再生装置との間で公開鍵暗号を用いた相互認証プロトコルを実行するセキュリティモジュールを有することを特徴とする情報記録媒体。

【請求項２１】　上記セキュリティモジュールは、上記相互認証プロトコルを実行するときに、情報記録／再生装置の識別情報がリボケーションリストに掲載されていないことを確認することを特徴とする請求項２０記載の情報記録媒体。

【請求項２２】　上記セキュリティモジュールは、自分と上記情報記録／再生装置の何れか一方若しくは両方がリボケーションリストを保持する保持手段を備えるか否かに応じた相互認証プロトコルを使用することを特徴とする請求項２０記載の情報記録媒体。

【請求項２３】　上記セキュリティモジュールは、上記相互認証プロトコルを実行するときに、自分が持つリボケーションリストのバージョンナンバーを情報記録／再生装置に送り、これと上記情報記録／再生装置が送ったリボケーションリストのバージョンナンバーを受信して比較し、自分のものの方が新しい場合にはリボケーションリストを相手に送り、相手のものの方が新しい場合には、相手から送られたリボケーションリストを現在自分が持っているものと置き換える処理を行うことを特徴とする請求項２０記載の情報記録媒体。

【請求項２４】　上記セキュリティモジュールは、自分と上記情報記録／再生装置が持つリボケーションリストのうち、新しいリボケーションリストを用いて、上記相互認証プロトコルを実行することを特徴とする請求項２３記載の情報記録媒体。

【請求項２５】　上記セキュリティモジュールは、上記相互認証プロトコルを実行するときに、情報記録／再生装置の識別情報がレジストレーションリストに

登録されていることを確認することを特徴とする請求項２０記載の情報記録媒体。

【請求項２６】　上記セキュリティモジュールは、自分と上記情報記録／再生装置の何れか一方若しくは両方がレジストレーションリストを保持する保持手段を備えるか否かに応じた相互認証プロトコルを使用することを特徴とする請求項２０記載の情報記録媒体。

【請求項２７】　上記セキュリティモジュールは、上記相互認証プロトコルを実行するときに、自分が持つレジストレーションリストのバージョンナンバーを情報記録／再生装置に送り、これと上記情報記録／再生装置が送ったレジストレーションリストのバージョンナンバーを受信して比較し、自分のものの方が新しい場合にはレジストレーションリストを相手に送り、相手のものの方が新しい場合には、相手から送られたレジストレーションリストを現在自分が持っているものと置き換える処理を行うことを特徴とする請求項２０記載の情報記録媒体。

【請求項２８】　上記セキュリティモジュールは、自分と上記情報記録／再生装置が持つレジストレーションリストのうち、新しいレジストレーションリストを用いて、上記相互認証プロトコルを実行することを特徴とする請求項２７記載の情報記録媒体。

【請求項２９】　上記セキュリティモジュールは、上記相互認証プロトコルを実行するときに、情報記録／再生装置の識別情報がリボケーションリストに掲載されていないこと、及び／又は、レジストレーションリストに登録されていることを確認することを特徴とする請求項２０記載の情報記録媒体。

【請求項３０】　上記セキュリティモジュールは、自分と上記情報記録／再生装置の何れか一方若しくは両方がリボケーションリスト及びレジストレーションリストを保持する保持手段を備えるか否かに応じた相互認証プロトコルを使用することを特徴とする請求項２０記載の情報記録媒体。

【請求項３１】　上記セキュリティモジュールは、上記相互認証プロトコルを実行するときに、自分が持つリボケーションリスト及びレジストレーションリストのバージョンナンバーを情報記録／再生装置に送り、これと上記情報記録／再生装置が送ったリボケーションリスト及びレジストレーションリストのバージョ

ンナンバーを受信して比較し、自分のものの方が新しい場合にはリボケーションリスト及びレジストレーションリストを相手に送り、相手のものの方が新しい場合には、相手から送られたリボケーションリスト及びレジストレーションリストを現在自分が持っているものと置き換える処理を行うことを特徴とする請求項２０記載の情報記録媒体。

【請求項３２】　上記セキュリティモジュールは、自分と上記情報記録／再生装置が持つリボケーションリスト及び／又はレジストレーションリストのうち、新しいリボケーションリスト及び／又はレジストレーションリストを用いて、上記相互認証プロトコルを実行することを特徴とする請求項３１記載の情報記録媒体。

~~【請求項３３】　上記セキュリティモジュールは、上記相互認証プロトコルの~~実行時に、リボケーションリストとレジストレーションリストのうち何れか一方を選択的に使用することを特徴とする請求項２０記載の情報記録媒体。

【請求項３４】　上記セキュリティモジュールが管理する暗号鍵を用いて暗号化されたデータを格納することを特徴とする請求項２０記載の情報記録媒体。

【請求項３５】　上記セキュリティモジュールは、データの記録時及び再生時に、情報記録／再生装置との間で公開鍵暗号を用いた鍵共有プロトコルを実行し、この際に共有した鍵を用いて、データを暗号化する暗号鍵を情報記録／再生装置に送信あるいは情報記録／再生装置から受信することを特徴とする請求項２０記載の情報記録媒体。

【請求項３６】　データの書き込み及び読み出しの処理が上記セキュリティモジュールを介して行われることを特徴とする請求項２０記載の情報記録媒体。

【請求項３７】　上記セキュリティモジュールは、データの記録時に、情報記録／再生装置との間で公開鍵暗号を用いた鍵共有プロトコルを実行し、この際に共有した鍵を用いて受信したデータを復号し、さらに別の鍵を用いてデータを暗号化することを特徴とする請求項３６記載の情報記録媒体。

【請求項３８】　データの再生時に、記録媒体からデータを読み出して暗号鍵１を用いて復号した後、情報記録／再生装置との間で公開鍵暗号を用いた鍵共有プロトコルを実行し、共有した鍵を用いてデータを暗号化して情報記録／再生装

置に送信することを特徴とする請求項３６記載の情報記録媒体。

【請求項３９】　データの記録時及び再生時に、情報記録媒体のセキュリティモジュールとの間で公開鍵暗号を用いた相互認証プロトコルを実行する制御手段を備えることを特徴とする情報記録／再生装置。

【請求項４０】　上記制御手段は、上記相互認証プロトコルを実行するときに、上記セキュリティモジュールの識別情報がリボケーションリストに掲載されていないことを確認することを特徴とする請求項３９記載の情報記録／再生装置。

【請求項４１】　上記制御手段は、上記セキュリティモジュールを有する情報記録媒体と自分の何れか一方若しくは両方がリボケーションリストを保持する保持手段を備えるか否かに応じた相互認証プロトコルを使用することを特徴とする請求項３９記載の情報記録／再生装置。

【請求項４２】　上記制御手段は、上記相互認証プロトコルを実行するときに、自分が持つリボケーションリストのバージョンナンバーをセキュリティモジュールに送り、これと上記セキュリティモジュールが送ったリボケーションリストのバージョンナンバーを受信して比較し、自分のものの方が新しい場合にはリボケーションリストを相手に送り、相手のものの方が新しい場合には、相手から送られたリボケーションリストを現在自分が持っているものと置き換える処理を行うことを特徴とする請求項３９記載の情報記録／再生装置。

【請求項４３】　上記制御手段は、自分と上記セキュリティモジュールの両者のもつリボケーションリストのうち、新しいリボケーションリストを用いて、上記相互認証プロトコルを実行することを特徴とする請求項４２記載の情報記録／再生装置。

【請求項４４】　上記制御手段は、上記相互認証プロトコルを実行するときに、上記セキュリティモジュールの識別情報がレジストレーションリストに登録されていることを確認することを特徴とする請求項３９記載の情報記録／再生装置。

【請求項４５】　上記制御手段は、上記セキュリティモジュールを有する情報記録媒体と自分の何れか一方若しくは両方がレジストレーションリストを保持する保持手段を備えるか否かに応じた相互認証プロトコルを使用することを特徴と

する請求項３９記載の情報記録／再生装置。

【請求項４６】　上記制御手段は、上記相互認証プロトコルを実行するときに、自分が持つレジストレーションリストのバージョンナンバーをセキュリティモジュールに送り、これと上記セキュリティモジュールが送ったレジストレーションリストのバージョンナンバーを受信して比較し、自分のものの方が新しい場合にはレジストレーションリストを相手に送り、相手のものの方が新しい場合には、相手から送られたレジストレーションリストを現在自分が持っているものと置き換える処理を行うことを特徴とする請求項３９記載の情報記録／再生装置。

【請求項４７】　上記制御手段は、自分と上記セキュリティモジュールの両者のもつレジストレーションリストのうち、新しいレジストレーションリストを用いて、上記相互認証プロトコルを実行することを特徴とする請求項４６記載の情報記録／再生装置。

【請求項４８】　上記制御手段は、上記相互認証プロトコルを実行するときに、上記セキュリティモジュールの識別情報がリボケーションリストに掲載されていないこと、及び／又は、レジストレーションリストに登録されていることを確認することを特徴とする請求項３９記載の情報記録／再生装置。

【請求項４９】　上記制御手段は、上記セキュリティモジュールを有する情報記録媒体と自分の何れか一方若しくは両方がリボケーションリスト及びレジストレーションリストを保持する保持手段を備えるか否かに応じた相互認証プロトコルを使用することを特徴とする請求項３９記載の情報記録／再生装置。

【請求項５０】　上記制御手段は、上記相互認証プロトコルを実行するときに、自分が持つリボケーションリスト及びレジストレーションリストのバージョンナンバーをセキュリティモジュールに送り、これと上記セキュリティモジュールが送ったリボケーションリスト及びレジストレーションリストのバージョンナンバーを受信して比較し、自分のものの方が新しい場合にはリボケーションリスト及びレジストレーションリストを相手に送り、相手のものの方が新しい場合には、相手から送られたリボケーションリスト及びレジストレーションリストを現在自分が持っているものと置き換える処理を行うことを特徴とする請求項３９記載の情報記録／再生装置。

【請求項５１】　上記制御手段は、自分と上記セキュリティモジュールの両者のもつリボケーションリスト及び／又はレジストレーションリストのうち、新しいリボケーションリスト及び／又はレジストレーションリストを用いて、上記相互認証プロトコルを実行することを特徴とする請求項５０記載の情報記録／再生装置。

【請求項５２】　上記セキュリティモジュールは、上記相互認証プロトコルの実行時に、リボケーションリストとレジストレーションリストのうち何れか一方を選択的に使用することを特徴とする請求項３９記載の情報記録／再生装置。

【請求項５３】　上記制御手段は、データの記録時及び再生時に、上記セキュリティモジュールとの間で公開鍵暗号を用いた鍵共有プロトコルを実行し、この際に共有した鍵を用いて、データを暗号化する暗号鍵を上記セキュリティモジュールに送信あるいは上記セキュリティモジュールから受信することを特徴とする請求項３９記載の情報記録／再生装置。

【請求項５４】　上記制御手段は、データの記録時に、上記セキュリティモジュールとの間で公開鍵暗号を用いた鍵共有プロトコルを実行し、この際に共有した鍵を用いてデータを暗号化して情報記録媒体に格納することを特徴とする請求項３９記載の情報記録／再生装置。

【請求項５５】　上記制御手段は、データの記録時に、上記セキュリティモジュールとの間で公開鍵暗号を用いた鍵共有プロトコルを実行し、この際に共有した鍵を用いてデータを暗号化して上記セキュリティモジュールに送信することを特徴とする請求項３９記載の情報記録／再生装置。

【請求項５６】　上記制御手段は、データの記録時に、上記セキュリティモジュールとの間で公開鍵暗号を用いた鍵共有プロトコルを実行し、この際に共有した鍵を用いてデータの暗号化に用いる暗号鍵を暗号化して上記セキュリティモジュールに送信し、又は共有した鍵を用いて暗号化された暗号鍵を上記セキュリティモジュールから受信し、上記暗号鍵を用いてデータを暗号化して上記セキュリティモジュールに送信することを特徴とする請求項３９記載の情報記録／再生装置。

【請求項５７】　上記制御手段は、データの再生時に、上記セキュリティモジュールとの間で公開鍵暗号を用いた鍵共有プロトコルを実行し、この際に共有した鍵を用いて、上記セキュリティモジュールから送られたデータを復号することを特徴とする請求項３９記載の情報記録／再生装置。

【請求項５８】　上記制御手段は、データの再生時に、上記セキュリティモジュールとの間で公開鍵暗号を用いた鍵共有プロトコルを実行し、この際に共有した鍵を用いて、データの暗号化に用いる暗号鍵を暗号化してセキュリティモジュールに送信し、又は共有した鍵を用いて暗号化された暗号鍵を上記セキュリティモジュールから受信し、上記暗号鍵を用いて上記セキュリティモジュールから送られたデータを復号することを特徴とする請求項３９記載の情報記録／再生装置。

【請求項５９】　情報記録／再生装置により情報記録媒体にデータを記録、あるいは情報記録媒体からデータを再生する情報記録／再生方法において、

情報記録媒体が有するセキュリティモジュールと情報記録／再生装置が公開鍵暗号を用いた相互認証プロトコルを実行するステップを有することを特徴とする情報記録／再生方法。

【請求項６０】　上記相互認証プロトコルを実行するときに、情報記録／再生装置とセキュリティモジュールが、互いに、他方の識別情報がリボケーションリストに掲載されていないことを確認するステップを有することを特徴とする請求項５９記載の情報記録／再生方法。

【請求項６１】　セキュリティモジュールと上記情報記録／再生装置の何れか一方若しくは両方がリボケーションリストを保持するか否かに応じた相互認証プロトコルを使用することを特徴とする請求項５９記載の情報記録／再生方法。

【請求項６２】　上記相互認証プロトコルを実行するときに、情報記録／再生装置とセキュリティモジュールが、互いに、自分が所有するリボケーションリストのバージョンナンバーを教えるステップと、新しいリボケーションリストを持つものがそれを他方に送るステップと、古いリボケーションリストを持つものは送られた新しいリボケーションリストを用いて自分のリボケーションリストを置き換えるステップを有することを特徴とする請求項５９記載の情報記録／再生方

法。

【請求項６３】　セキュリティモジュールと上記情報記録／再生装置が持つリボケーションリストのうち、新しいリボケーションリストを用いて、上記相互認証プロトコルを実行することを特徴とする請求項６２記載の情報記録／再生方法。

【請求項６４】　上記相互認証プロトコルを実行するときに、情報記録／再生装置とセキュリティモジュールが、互いに、他方の識別情報がレジストレーションリストに掲載されていないことを確認するステップを有することを特徴とする請求項５９記載の情報記録／再生方法。

【請求項６５】　セキュリティモジュールと上記情報記録／再生装置の何れか一方若しくは両方がレジストレーションリストを保持するか否かに応じた相互認証プロトコルを使用することを特徴とする請求項５９記載の情報記録／再生方法。

【請求項６６】　上記相互認証プロトコルを実行するときに、情報記録／再生装置とセキュリティモジュールが、互いに、自分が所有するレジストレーションリストのバージョンナンバーを教えるステップと、新しいレジストレーションリストを持つものがそれを他方に送るステップと、古いレジストレーションリストを持つものは送られた新しいレジストレーションリストを用いて自分のレジストレーションリストを置き換えるステップを有することを特徴とする請求項５９記載の情報記録／再生方法。

【請求項６７】　セキュリティモジュールと上記情報記録／再生装置が持つレジストレーションリストのうち、新しいレジストレーションリストを用いて、上記相互認証プロトコルを実行することを特徴とする請求項６６記載の情報記録／再生方法。

【請求項６８】　上記相互認証プロトコルを実行するときに、情報記録／再生装置とセキュリティモジュールが、互いに、他方の識別情報がリボケーションリストに掲載されていないこと、及び／又は、レジストレーションリストに掲載されていないことを確認するステップを有することを特徴とする請求項５９記載の情報記録／再生方法。

【請求項６９】　セキュリティモジュールと上記情報記録／再生装置の何れか一方若しくは両方がリボケーションリスト及びレジストレーションリストを保持するか否かに応じた相互認証プロトコルを使用することを特徴とする請求項５９記載の情報記録／再生方法。

【請求項７０】　上記相互認証プロトコルを実行するときに、情報記録／再生装置とセキュリティモジュールが、互いに、自分が所有するリボケーションリスト及びレジストレーションリストのバージョンナンバーを教えるステップと、新しいリボケーションリスト及びレジストレーションリストを持つものがそれを他方に送るステップと、古いリボケーションリスト及びレジストレーションリストを持つものは送られた新しいリボケーションリスト及びレジストレーションリストを用いて自分のリボケーションリスト及びレジストレーションリストを置き換えるステップを有することを特徴とする請求項５９記載の情報記録／再生方法。

【請求項７１】　セキュリティモジュールと上記情報記録／再生装置が持つリボケーションリスト及び／又はレジストレーションリストのうち、新しいリボケーションリスト及び／又はレジストレーションリストを用いて、上記相互認証プロトコルを実行することを特徴とする請求項７０記載の情報記録／再生方法。

【請求項７２】　セキュリティモジュールと上記情報記録／再生装置は、上記相互認証プロトコルの実行時に、リボケーションリストとレジストレーションリストのうち何れか一方を選択的に使用することを特徴とする請求項５９記載の情報記録／再生方法。

【請求項７３】　データの記録時又は再生時に、情報記録／再生装置とセキュリティモジュールが公開鍵暗号を用いた鍵共有プロトコルを実行するステップと、共有された鍵を用いてデータを暗号化する暗号鍵を一方が暗号化して他方に送るステップを有することを特徴とする請求項５９記載の情報記録／再生方法。

【請求項７４】　データの記録時又は再生時に、情報記録／再生装置とセキュリティモジュールが公開鍵暗号を用いた鍵共有プロトコルを行うステップと、共有された鍵を用いてデータを一方が暗号化して他方に送るステップを有することを特徴とする請求項５９記載の情報記録／再生方法。

【請求項７５】　データの記録時に、情報記録／再生装置とセキュリティモジュールが公開鍵暗号を用いた鍵共有プロトコルを実行するステップと、共有された鍵を用いてデータを情報記録／再生装置が暗号化して他方に送るステップと、セキュリティモジュールが受信したデータを共有された鍵を用いて復号するステップと、セキュリティモジュールが上記復号したデータを鍵を用いて暗号化するステップと、セキュリティモジュールが上記暗号化したデータを情報記録媒体に格納するステップを有することを特徴とする請求項５９記載の情報記録／再生方法。

【請求項７６】　データの再生時に、情報記録／再生装置とセキュリティモジュールが公開鍵暗号を用いた鍵共有プロトコルを行つて鍵を共有するステップと、

セキュリティモジュールが情報記録媒体からデータを読み出して鍵を用いて復号するステップと、セキュリティモジュールが上記復号後のデータを共有した鍵を用いて暗号化するステップと、セキュリティモジュールが上記暗号化後のデータを情報記録／再生装置に送信するステップとを有することを特徴とする請求項５９記載の情報記録／再生方法。

【請求項７７】　外部装置とインターフェースをとるためのインターフェース機能と、乱数を生成するための乱数生成機能と、情報を保存するための記憶機能と、公開鍵暗号技術を用いた相互認証プロトコルに必要な計算を行う演算機能を有するセキュリティモジュールを備えることを特徴とする情報記録媒体。

【請求項７８】　上記セキュリティモジュールは、データを記録するための記録領域にアクセスするためのインターフェース機能を備えることを特徴とする請求項７７記載の情報記録媒体。

【請求項７９】　セキュリティモジュールを有する情報記録媒体を製造する記録媒体製造装置であって、

最新のリボケーションリスト及び／又はレジストレーションリストを上記情報記録媒体に記録する記録手段を備える

ことを特徴とする記録媒体製造装置。

【請求項８０】　上記情報記録媒体のセキュリティモジュールが上記リボケーションリスト及び／又はレジストレーションリストを保持するのに十分な保持手段を備えるとき、

上記記録手段は、上記保持手段に上記最新のリボケーションリスト及び／又はレジストレーションリストを記録することを特徴とする請求項７９記載の記録媒体製造装置。

【請求項８１】　上記情報記録媒体のセキュリティモジュールが上記リボケーションリスト及び／又はレジストレーションリストを保持するのに十分な保持手段を備えないとき、

上記記録手段は、上記情報記録媒体のデータ記録領域に上記最新のリボケーションリスト及び／又はレジストレーションリストを記録することを特徴とする請求項７９記載の記録媒体製造装置。

【請求項８２】　上記最新のリボケーションリスト及び／又はレジストレーションリストを格納する格納手段を備えることを特徴とする請求項７９記載の記録媒体製造装置。

【請求項８３】　外部から上記最新のリボケーションリスト及び／又はレジストレーションリストを入手する入手手段を備えることを特徴とする請求項７９記載の記録媒体製造装置。

【請求項８４】　セキュリティモジュールを有する情報記録媒体を製造する記録媒体製造方法であって、

最新のリボケーションリスト及び／又はレジストレーションリストを上記情報記録媒体に記録するステップを有する

ことを特徴とする記録媒体製造方法。

【請求項８５】　上記情報記録媒体のセキュリティモジュールが上記リボケーションリスト及び／又はレジストレーションリストを保持するのに十分な保持手段を備えるとき、

上記保持手段に上記最新のリボケーションリスト及び／又はレジストレーションリストを記録することを特徴とする請求項８４記載の記録媒体製造方法。

【請求項８６】　上記情報記録媒体のセキュリティモジュールが上記リボケーションリスト及び／又はレジストレーションリストを保持するのに十分な保持手段を備えないとき、

上記情報記録媒体のデータ記録領域に上記最新のリボケーションリスト及び／又はレジストレーションリストを記録することを特徴とする請求項８４記載の記録媒体製造方法。

【請求項８７】　上記最新のリボケーションリスト及び／又はレジストレーションリストを格納するステップを有することを特徴とする請求項８４記載の記録媒体製造方法。

【請求項８８】　外部から上記最新のリボケーションリスト及び／又はレジストレーションリストを入手するステップを有することを特徴とする請求項８４記載の記録媒体製造方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、安全にデータを授受することを可能にした情報記録／再生システム、情報記録／再生装置及び方法、情報記録媒体、記録媒体製造装置及び方法に関する。

【０００２】

【従来の技術】

近年は、情報をデジタル的に記録する記録装置及び記録媒体が普及しつつある。これらの記録装置及び記録媒体は、例えば、映像や音楽のデータを劣化させることなく記録し、再生するので、データを、その質を維持しながら何度もコピーすることができる。しかしながら、映像や音楽のデータの著作権者にしてみれば、自らが著作権を有するデータが、その質を維持しながら何度も不正にコピーされ、市場に流通してしまう恐れがある。このため、記録装置及び記録媒体の側で、著作権を有するデータが不正にコピーされるのを防ぐ必要がある。

【０００３】

このような著作権保護のための手法として、例えば、ミニディスク（MD）（商

標）システムにおいては、いわゆるＳＣＭＳ(Serial Copy Management System)と呼ばれる方法が用いられている。当該ＳＣＭＳの情報は、デジタルインターフェースによって、音楽データとともに伝送される情報であり、この情報は、音楽データがコピーフリー（以下、copy freeと記す）であるか、又は、１回のみコピーを許す（以下、copy once allowedと記す）データであるか、コピーが禁止されている（以下、copy prohibitedと記す）データであるかのうちのいずれのデータであるのかを表す。ミニディスクレコーダは、デジタルインターフェースから音楽データを受信した場合、上記ＳＣＭＳの情報を検出し、これがcopy prohibitedであれば、音楽データをミニディスクに記録せず、copy once allowedであれば、当該ＳＣＭＳの情報をcopy prohibitedに変更して受信した音楽データとともに記録し、copy freeであれば、当該ＳＣＭＳの情報をそのまま、受信した音楽データとともに記録する。

【０００４】

このように、ミニディスクシステムにおいては、ＳＣＭＳの情報を用いて、著作権を有するデータが不正にコピーされるのを防いでいる。

【０００５】

また、著作権を有するデータが不正にコピーされるのを防ぐ別の例としては、デジタルバーサタイルディスク（Digital Versatile Disk：DVD（商標））システムにおける、コンテンツスクランブルシステムが挙げられる。このシステムでは、ディスク上の著作権を有するデータが全て暗号化され、ライセンスを受けた記録装置だけが暗号鍵を与えられ、これにより上記暗号化されているデータを復号し、意味のあるデータを得ることができるようになされている。そして、記録装置は、ライセンスを受ける際に、不正コピーを行わない等の動作規定に従うように設計される。このようにして、ＤＶＤシステムにおいては、著作権を有するデータが不正にコピーされるのを防いでいる。

【０００６】

【発明が解決しようとする課題】

しかしながら、上記のミニディスクシステムが採用している方式では、ＳＣＭＳがcopy once allowedであれば、これをcopy prohibitedに変更し、受信したデ

ータとともに記録するなどの動作規定に従わない記録装置が、不正に製造されてしまう虞がある。

【０００７】

また、上記のＤＶＤシステムが採用している方式では、再生のみ可能なＲＯＭメディアに対しては有効であるが、ユーザがデータを記録可能なＲＡＭメディアにおいては有効ではない。すなわち、ＲＡＭメディアにおいては、不正者は、暗号を解読できない場合であっても、ディスク上のデータを全部、新しいディスクに不正にコピーすることによって、ライセンスを受けた正当な記録装置で動作するディスクを新たに作ることができるからである。

【０００８】

このようなことから、本件出願人は、先に出願した特願平１０－２５３１０号の特許出願において、個々の記録媒体を識別するための情報（以下、媒体識別情報と呼ぶ）を記録媒体に持たせ、この情報はライセンスを受けた装置しかアクセスできないようにすることにより、不正コピーを防止する技術を提案している。すなわち、当該技術においては、記録媒体上のデータを、ライセンスを受けることによって得られる秘密に基づく鍵と媒体識別情報の両方を用いて暗号化することにより、ライセンスを受けていない装置がデータを読み出しても意味のないものとしている。さらに、当該技術によれば、装置にライセンスを与える際にその装置の動作を規定し、不正コピーを行わないようにもしている。このように、上記技術によれば、ライセンスを得ていない装置は媒体識別情報にアクセスできず、また媒体識別情報は個々の媒体毎に個別の値になっているため、例えばライセンスを受けていない装置がアクセス可能なすべての情報を新たな媒体にコピーしたとしても、そのようにして作られた媒体は、ライセンスを受けていない装置でもライセンスを受けた装置でも正しく情報が読み出せないことになり、不正コピーの防止が実現されている。

【０００９】

しかしながら、上記技術においては、ある記録装置によって情報が記録された記録媒体を他の装置にて再生できることを保証するために、記録媒体上のデータを暗号化するための暗号鍵は、システム全体で共通の秘密鍵（マスターキー）に

基づいて生成されるようになっている。これはすなわち、例えば正当な一つの装置が解析されて不正にマスターキーが盗まれてしまうようなことが起きると、そのシステムの任意の装置によって記録されたすべてのデータの暗号が解かれ、システム全体が壊滅する恐れがあることを意味している。

【００１０】

そこで、本発明の目的は、暗号鍵を安全に保管することができるようにした情報記録／再生システム、情報記録／再生装置、情報記録／再生方法、情報記録媒体、及び情報記録媒体製造装置及び方法を提供することにある。

【００１１】

また、本発明の他の目的は、不正な機器にデータを漏らすことのないように、或いは正当な機器のみにデータを供給できるようにした情報記録／再生システム、情報記録／再生装置及び方法、情報記録媒体、記録媒体製造装置及び方法を提供することにある。

【００１２】

また、本発明の他の目的は、正当な機器ではあるが、例えば不正な解析により当該機器の秘密が露呈してしまったような場合に、当該機器に対して新たにデータを与えてしまうことをも防ぐことができるようにした、情報記録／再生システム、情報記録／再生装置及び方法、情報記録媒体、記録媒体製造装置及び方法を提供することにある。

【００１３】

さらに、本発明の他の目的は、映画や音楽などの著作権があるデータの不正な（著作権者の意に反する）複製を防ぐことができるようにした情報記録／再生システム、情報記録／再生装置及び方法、情報記録媒体、記録媒体製造装置及び方法を提供することにある。

【００１４】

【課題を解決するための手段】

本発明では、情報記録媒体にセキュリティモジュールを持たせる。情報記録媒体上に記録されるデータは、個々のデータ毎に異なる暗号鍵で暗号化され、暗号鍵はセキュリティモジュールが安全に保管する。また、セキュリティモジュール

は記録／再生装置と公開鍵暗号技術を用いた相互記証を行い、相手が正当なライセンスを受けた装置であることを確認した上で、暗号鍵を装置に対して与えることにより、不正な装置にはデータを漏らさないようにする。さらに、信頼できるセンタが発行するリボケーションリスト及び／又はレジストレーションリストを活用することにより、正当な機器ではあるが不正な解析によって当該機器の秘密が露呈してしまったような場合に、その装置に新たにデータを与えてしまうことをも防ぐことができるようにする。

【００１５】

すなわち、本発明に係る情報記録／再生システムは、セキュリティモジュールを有する情報記録媒体と、上記セキュリティモジュールが管理する暗号鍵によって暗号化されたデータを上記情報記録媒体に記録、あるいは、上記セキュリティモジュールが管理する暗号鍵によって暗号化されたデータを上記情報記録媒体から再生する情報記録／再生装置とを備え、情報記録時、又は情報再生時に上記情報記録／再生装置とセキュリティモジュールとが公開鍵暗号技術を用いた相互認証プロトコルを実行することにより、上述した課題を解決する。

【００１６】

また、本発明に係る情報記録媒体は、データの記録時及び再生時に、情報記録／再生装置との間で公開鍵暗号を用いた相互認証プロトコルを実行するセキュリティモジュールを有することにより、上述した課題を解決する。

【００１７】

また、本発明に係る情報記録／再生装置は、データの記録時及び再生時に、情報記録媒体のセキュリティモジュールとの間で公開鍵暗号を用いた相互認証プロトコルを実行する制御手段を備えることにより、上述した課題を解決する。

【００１８】

また、本発明は、情報記録／再生装置により情報記録媒体にデータを記録、あるいは情報記録媒体からデータを再生する情報記録／再生方法において、情報記録媒体が有するセキュリティモジュールと情報記録／再生装置が公開鍵暗号を用いた相互認証プロトコルを実行するステップを有することにより、上述した課題を解決する。

【００１９】

さらに、本発明に係る情報記録媒体は、外部装置とインターフェースをとるためのインターフェース機能と、乱数を生成するための乱数生成機能と、情報を保存するための記憶機能と、公開鍵暗号技術を用いた相互認証プロトコルに必要な計算を行う演算機能を有するセキュリティモジュールを備えることにより、上述した課題を解決する。

【００２０】

また、本発明の記録媒体製造装置は、セキュリティモジュールを有する情報記録媒体を製造する記録媒体製造装置であって、最新のリボケーションリスト及び／又はレジストレーションリストを上記情報記録媒体に記録する記録手段を備えることにより、上述した課題を解決する。

【００２１】

また、本発明の記録媒体製造方法は、セキュリティモジュールを有する情報記録媒体を製造する記録媒体製造方法であって、最新のリボケーションリスト及び／又はレジストレーションリストを上記情報記録媒体に記録するステップを有することにより、上述した課題を解決する。

【００２２】

【発明の実施の形態】

以下、本発明の実施の形態について、図面を参照しながら詳細に説明する。

【００２３】

図１には、本発明の第１の実施の形態に係る情報記録媒体の一例としての光ディスク情報記録媒体１０の構成例を示す。

【００２４】

この光ディスク情報記録媒体１０は、カートリッジ１１内に、データを記録する光ディスク１２と、不揮発性メモリ３４を有するセキュリティモジュール１３とを備えている。図２は、当該第１の実施の形態において不揮発性メモリ３４を有するセキュリティモジュール１３の構成例を示している。

【００２５】

セキュリティモジュール１３は、図２に示すように、当該モジュール外の装置

とデータの授受をするための接触式あるいは非接触式のインターフェース部３１と、各種の演算を行うための演算部３２と、乱数発生部３３と、不揮発性メモリ３４と、それらを制御するための制御部３５とを備えている。

【００２６】

図３は、本発明の第１の実施の形態としての光ディスク記録再生装置１００の構成例を示している。

【００２７】

この光ディスク記録再生装置１００は、上記光ディスク情報記録媒体１０を使用してデータの記録／再生を行うものであり、カートリッジ１１内の光ディスク１２を回転させるスピンドルモータ１０１、光学ヘッド１０２、サーボ回路１０３、記録／再生回路１０４、これらを制御する制御部１０５、この制御部１０５に接続された入力部１０６、乱数を発生する乱数発生部１０７、不揮発性メモリ１１０、インターフェース部１０８などを備えている。

【００２８】

スピンドルモータ１０１は、サーボ回路１０３によってその回転動作が制御され、光ディスク１２を回転させる。光学ヘッド１０２は、レーザビームを光ディスク１２の記録面に照射することで、データの記録／再生を行う。サーボ回路１０３は、スピンドルモータ１０１を駆動することにより、光ディスク１２を所定の速度で（例えば線速度一定で）回転させる。また、サーボ回路１０３は、光学ヘッド１０２による光ディスク１２へのトラッキング及びフォーカシングの他、上記光学ヘッド１０２をディスク半径方向に移動させる際のスレッドサーボ制御を行う。

【００２９】

そして、記録／再生回路１０４は、制御部１０５により動作モードが切り換えられる暗号化部１０４Ａと復号部１０４Ｂを有する。暗号化部１０４Ａは、記録モード時に、外部から記録信号の供給を受けると、その記録信号を暗号化し、光学ヘッド１０２に供給して、光ディスク１２に記録させる。復号部１０４Ｂは、再生モード時に、光学ヘッド１０２により光ディスク１２から再生されたデータを復号し、外部に再生信号として出力する。

【００３０】

また、入力部１０６は、ボタン、スイッチ、リモートコントローラなどにより構成され、ユーザにより入力操作がなされたとき、その入力操作に対応する信号を出力する。制御部１０５は、記憶されている所定のコンピュータプログラムに従って、装置全体を制御する。乱数発生部１０７は、制御部１０５の制御により、所定の乱数を発生する。インターフェース１０８部は、接触式あるいは非接触式であり、情報記録媒体１０のセキュリティモジュール１３との間でデータの授受を行う。

【００３１】

さらに、この第１の実施の形態の光ディスク記録再生装置１００は、演算部１０９と不揮発性メモリ１１０を備えている。

【００３２】

ここで、本発明の第１の実施の形態において、上記光ディスク情報記録媒体１０のセキュリティモジュール１３は、個別の（１つの媒体毎）識別コード（ＩＤ)と、当該ＩＤに対応する公開鍵暗号系の秘密鍵と公開鍵、さらに信頼できるセンタ（Trusted Center:TC、以下、単にセンタＴＣと呼ぶ）から公開鍵証明書が与えられており、それら情報を不揮発性メモリ３４或いは当該不揮発性メモリ３４とは別の不揮発性の記憶領域に格納している。同じく、この第１の実施の形態の光ディスク記録再生装置１００は、個別の（１台の装置毎の）識別コード（ＩＤ)と、当該ＩＤに対応する公開鍵暗号系の秘密鍵と公開鍵、センタＴＣから公開鍵証明書が与えられており、これら情報を不揮発性メモリ１１０或いは当該不揮発性メモリ１１０とは別の不揮発性の記憶領域に格納している。特に、秘密鍵は外部に漏れないように、それぞれ不揮発性メモリ３４，１１０或いはそれらとは別の記憶領域において安全に格納する。

【００３３】

上記光ディスク情報記録媒体１０のセキュリティモジュール１３に与えられている上記公開鍵証明書は、当該光ディスク情報記録媒体１０のＩＤと公開鍵を含む情報に、センタＴＣがデジタル署名を施したデータである。同様に、光ディスク記録再生装置１００に与えられている公開鍵証明書は、当該光ディスク記録再

生装置１００のＩＤと公開鍵を含む情報に、センタＴＣがデジタル署名を施したデータである。すなわち、これら公開鍵証明書は、個々の光ディスク情報記録媒体、及び、個々の光ディスク記録再生装置が、それぞれ正当なものであることをセンタＴＣが認めることを証明する文書であり、通常は、各記録媒体、装置がそれぞれ出荷される時に、センタＴＣから与えられるものである。なお、上記デジタル署名技術とは、あるデータを生成したのが、あるユーザであることを証明できる技術であり、例えばＩＥＥＥ　Ｐ１３６３で使用されているいわゆるＥＣ－ＤＳＡ（Elliptic Curve Digital Signature Algorithm）方式などがよく知られている。

【００３４】

上記公開鍵証明書には、図４に示すように、エンティティＩＤ（Entity ID）、エンティティ公開鍵（Entity Public Key）、センタＴＣのデジタル署名の各項目が含まれる。なお、上記エンティティ（Entity）とは、本発明実施の形態の情報記録媒体または記録再生装置を指す。上記エンティティＩＤはそのエンティティに個別に与えられた識別番号である。また、各エンティティには、公開鍵と秘密鍵のペアも個別に与えられ、そのうち公開鍵は上記公開鍵証明書に書かれ、秘密鍵はそのエンティティが秘密に保持する。また、エンティティタイプ（Entity Type）とは、情報記録媒体又は記録再生装置が後述するリボケーションリスト（或いは後の第２の実施の形態で説明するレジストレーションリスト）等を格納するための不揮発性メモリを備えたタイプであるか、或いは当該リストを格納するための不揮発性メモリを備えていないタイプであるかや、記録媒体の物理的構造を区別するための識別符号である。

【００３５】

また、この第１の実施の形態において、光ディスク情報記録媒体１０の不揮発性メモリ３４と光ディスク記録再生装置１００の不揮発性メモリ１１０には、それぞれ上記公開鍵証明書に含まれる上記センタＴＣのデジタル署名を検証するために、システム全体で共通であるセンタＴＣの公開鍵がそれぞれ格納されている。

【００３６】

さらに、当該第１の実施の形態において、光ディスク情報記録媒体１０のセキュリティモジュール１３の不揮発性メモリ３４と、光ディスク記録再生装置１００の不揮発性メモリ１１０には、図５に示すリボケーションリストを格納する領域がそれぞれ設けられている。

【００３７】

上記リボケーションリストは、単調増加する番号であって当該リボケーションリストのバージョンを示すバージョンナンバーと、秘密鍵が露呈してしまった光ディスク情報記録媒体或いは光ディスク記録再生装置のＩＤ（リボークされる機器又は媒体のＩＤ）のリストと、センタＴＣによるデジタル署名とからなるものである。すなわち、リボケーションリストは、不正者リスト或いはブラックリストとも呼ばれ、本実施の形態のような光ディスク情報記録媒体や光ディスク記録再生装置等から成るシステム全体においてその記録媒体又は装置の秘密鍵が露呈してしまったものＩＤがリストアップされ、それに対し信頼できるセンタＴＣがデジタル署名を施したものである。したがって、あるエンティティ（情報記録媒体または記録再生装置）において、通信相手方の記録媒体若しくは装置のＩＤが当該リボケーションリストに載っていることを確認した場合、そのエンティティは通信相手方を不正なものと判断し、それ以上プロトコルを進めないようにすることができる。このことにより、秘密鍵が露呈してしまった記録媒体又は装置、及びそれを用いて不正に複製された記録媒体又は不正に製造された装置を、このシステムから排除することが可能になる。また、光ディスク記録再生装置１００を工場から出荷する際には、最新版のリボケーションリストを不揮発性メモリ１１０に格納して出荷する。

【００３８】

次に、図６から図８を用いて、第１の実施の形態の光ディスク記録再生装置１００が光ディスク情報記録媒体１０にデータを記録する手順を説明する。

【００３９】

なお、上述したように、第１の実施の形態の光ディスク記録再生装置１００は、センタＴＣから与えられたＩＤ、公開鍵暗号系の秘密鍵、公開鍵、公開鍵証明

書、及びリボケーションリストを上記不揮発性メモリ１１０に格納しており、また同様に、当該第１の実施の形態の光ディスク情報記録媒体１０のセキュリティモジュール１３は、センタＴＣから与えられたＩＤ、公開鍵暗号系の秘密鍵、公開鍵、公開鍵証明書、及びリボケーションリストを上記不揮発性メモリ３４に格納している。

【００４０】

先ず、図６において、光ディスク記録再生装置１００は、手順Ｒ１として、光ディスク情報記録媒体１０のセキュリティモジュール１３に対して、これからデータの記録を行うことを示す記録コマンド（記録開始コマンド）と、１回１回の記録を識別するために個別に割り当てるレコーディングＩＤ（Recording-ID）とを送る。

【００４１】

次に、手順Ｒ２として、光ディスク記録再生装置１００及び光ディスク情報記録媒体１０のセキュリティモジュール１３は、上記記録コマンドをトリガーとして、公開鍵暗号技術を用いた相互認証及び鍵共有プロトコルを実行する。

【００４２】

ここで、公開鍵暗号技術を用いた相互認証プロトコルは、相手側が正しい（センタＴＣから承認を得た）公開鍵と秘密鍵のペアを持っていることを互いに確認するプロトコルであり、例えばＩＥＥＥ　Ｐ１３６３で規格化作業中のＥＣ－ＤＳＡ（Elliptic Curve Digital Signature Algorithm）を用いることによって構成することができる。

【００４３】

なお、上記公開鍵暗号技術を用いた相互認証プロトコルにおいては、光ディスク情報記録媒体１０のセキュリティモジュール１３と光ディスク記録再生装置１００の双方が、それぞれ乱数発生機能（セキュリティモジュール１３の乱数発生部３３、装置１００の乱数発生部１０７）を用いて乱数を発生させること、不揮発性メモリに格納されている自己の秘密鍵及び公開鍵証明書を読み出すこと、公開鍵暗号技術に基づく演算を演算機能（演算部）で行うこと、が必要となる。

【００４４】

また、公開鍵暗号技術を用いた相互認証プロトコルに対し、共通鍵暗号技術を用いた相互認証プロトコルも広く知られているが、当該相互認証プロトコルはその名の通り、プロトコルを実行する２者が共通の鍵を持っていることを前提とするプロトコルである。共通鍵暗号技術を用いた相互認証プロトコルを採用しようとした場合、記録媒体と記録再生装置のインターオペラビリティを確保する必要があるため、システム全体で共通の鍵をすべてのセキュリティモジュール１３と光ディスク記録再生装置１００が持つ必要がある。但し、この場合、一つのセキュリティモジュールあるいは光ディスク記録再生装置が攻撃を受けて（解析されて）鍵が露呈してしまうと、その影響がシステム全体に広まってしまうという問題がある。

【００４５】

これに対し、公開鍵暗号技術を用いた相互認証プロトコルにおいては、各装置及び各セキュリティモジュールが持つ鍵は個別であり、しかも本実施の形態では上述したリボケーションリストを使用できるため、一つの装置或いは記録媒体の鍵が露呈したとしても、その装置或いは記録媒体だけをシステムから排除することができるので、影響を小さく抑えられるという利点がある。

【００４６】

上記公開鍵暗号技術を用いた鍵共有プロトコルは、２者間で安全に秘密情報を共有するためのプロトコルであり、やはりＩＥＥＥ　Ｐ１３６３で規格化作業中のいわゆるＥＣ－ＤＨ（Elliptic Curve Diffie Hellman）を用いることによって構成することができる。

【００４７】

公開鍵暗号技術を用いた相互認証及び鍵共有プロトコルを実際に用いている例としては、ＩＥＥＥ　１３９４バス上のコンテンツプロテクション方式の一つである、ソニー、松下、日立、東芝、インテルの５社によって開発された、いわゆるＤＴＣＰ（Digital Transmission Content Protection）規格（この規格そのものはライセンスを受けないと見ることができないが、その概要を記したWhite Paper或いは規格のInformational versionを、ライセンス組織であるいわゆるＤ

ＴＬＡ（Digital Transmission Licensing Administrator）のウェブページであるhttp://www.dtcp.comから誰でも取得することが可能である）のＦＡＫＥ（Full Authentication and Key Exchange）プロトコルを挙げることができる。このプロトコルは、おおまかには下記のステップで構成される。

【００４８】

すなわち、当該プロトコルでは、先ず第１のステップとして、乱数発生器を用いて乱数を発生させ、不揮発性メモリから読み出した自分の公開鍵証明書とともに他方に送る。

【００４９】

次に、当該プロトコルでは、第２のステップとして、相手の公開鍵証明書の正当性を公開鍵暗号技術に基づく演算を行って確かめる。

【００５０】

次に、当該プロトコルでは、第３のステップとして、鍵共有のための、公開鍵暗号技術に基づく演算（第１段階）を行い、公開鍵暗号技術に基づく演算を行って作成した自分のデジタル署名文とともに相手に送る。

【００５１】

その後、当該プロトコルでは、第４のステップとして、相手から送られた第３のステップでのデータについて、公開鍵暗号技術に基づく演算を行って相手のデジタル署名の検証を行い、鍵共有のための、公開鍵暗号技術に基づく演算（第２段階）を行って共有鍵の値を計算する。

【００５２】

本方式においては、上記相互認証を行う際に、相手の装置が正しい秘密鍵と公開鍵のペアを持っていることのみならず、自分が持つリボケーションリストに相手の装置のＩＤが掲載されていないことを確認する。すなわち、出荷時には正当に鍵を持っていたが、それが例えばいわゆるリバースエンジニアリングなどの攻撃（不正な解析）を受け、鍵が露呈してしまった装置のＩＤが上記リボケーションリストに載せられているような場合には、当該リボケーションリストに載せられている装置（データを渡してはいけない装置）に対してデータを渡さずに済むようになる。

【００５３】

図６に戻り、さらに、上記手順Ｒ２では、記録再生装置と記録媒体のセキュリティモジュールとの間で、それぞれ自分が持っているリボケーションリストのバージョンナンバーを交換する。

【００５４】

次に、手順Ｒ３，Ｒ４として、もし何れかの一方が他方のリボケーションリストより新しいリボケーションリストを持っていた場合、当該新しいリボケーションリストを持っている方は自分のリボケーションリストを他方に送る。一方、古いリボケーションリストを持っている方は、新しいリボケーションリストを持っている方から、当該新しいリボケーションリストを送ってもらい、その正当性を検証した後、自分が持つリボケーションリストを、その送られてきた新しいリボケーションリストに更新する。すなわち、手順Ｒ３には、セキュリティモジュール上のリボケーションリストのバージョンが、記録再生装置上のリボケーションリストのバージョンよりも新しい場合におけるリボケーションリストの流れを示しており、また、手順Ｒ４には、記録再生装置上のリボケーションリストのバージョンが、セキュリティモジュール上のリボケーションリストのバージョンよりも新しい場合におけるリボケーションリストの流れを示している。

【００５５】

なお、手順Ｒ３，Ｒ４におけるリボケーションリストの送付は、後の手順Ｒ５におけるデータの記録と順序が前後してもかまわない。つまり、手順Ｒ５にてデータの記録を行った後に、手順Ｒ３或いはＲ４でのリボケーションリストの送付を行うようにしてもよい。

【００５６】

さてここで、上述したような公開鍵暗号技術を用いた相互認証及び鍵共有プロトコルの結果、光ディスク記録再生装置１００とセキュリティモジュール１３は、安全に、ある値を共有することになる。以下、この共有される値をセッション鍵（Session key：Kse）と呼ぶことにする。

【００５７】

次に、データを暗号化する暗号鍵（Content key：Kco）を決定するが、その決

定方法としては、例えば、以下に述べる暗号鍵決定方法（１）～暗号鍵決定方法（２）のうちの一つを用いればよい。

【００５８】

暗号鍵決定方法（１）では、Ｋse＝Ｋcoとする。すなわち、セッション鍵Ｋseを暗号鍵Ｋcoとする。この時、セキュリティモジュール１３は、暗号鍵Ｋcoを安全にその内部の不揮発性メモリ３４に格納するか、セキュリティモジュール１３が予め格納しているストレージ鍵（Storage key：Kst）を用いて当該暗号鍵Ｋcoを暗号化した値Ｅnc（Kst，Kco）を光ディスク記録再生装置１００に送り、光ディスク１２に記録させる。

暗号鍵決定方法（２）では、セキュリティモジュール１３が予め格納しているストレージ鍵Ｋstを暗号鍵Ｋcoとする。この場合、セキュリティモジュール１３がストレージ鍵Ｋstを上記セッション鍵Ｋseで暗号化して光ディスク記録再生装置１００に送り、ストレージ鍵Ｋst（＝ｋco）を用いてデータを暗号化して光ディスク１２に記録させる。

暗号鍵決定方法（３）では、セキュリティモジュール１３がそのデータ用の暗号鍵Ｋcoを乱数発生器などを用いて新たに発生させる。この場合、セキュリティモジュール１３が当該暗号鍵Ｋcoを上記セッション鍵Ｋseで暗号化して光ディスク記録再生装置１００に送り、この装置１００において当該暗号鍵Ｋcoを用いてデータを暗号化して光ディスク１２に記録させる。セキュリティモジュール１３は、暗号鍵Ｋcoを安全にその内部の不揮発性メモリ３４に格納するか、セキュリティモジュール１３が予め格納しているストレージ鍵Ｋstを用いて上記暗号鍵Ｋcoを暗号化した値Ｅnc（Kst，Kco）を光ディスク記録再生装置１００に送り、光ディスク１２に記録させる。

暗号鍵決定方法（４）では、光ディスク記録再生装置１００がそのデータ用の暗号鍵Ｋcoを乱数発生器などを用いて新たに発生させ、当該暗号鍵Ｋcoによりデータを暗号化して記録する。この場合、光ディスク記録再生装置１００が暗号鍵Ｋcoをセッション鍵Ｋseで暗号化してセキュリティモジュール１３に送る。セキュリティモジュール１３は暗号鍵Ｋcoを安全にその内部の不揮発性メモリ３４に格納するか、セキュリティモジュール１３が予め格納しているストレージ鍵Ｋst

を用いて暗号鍵Ｋcoを暗号化した値Ｅnc（Kst，Kco）を光ディスク記録再生装置１００に送り、光ディスク１３に記録させる。

【００５９】

上述した暗号鍵決定方法（１）～（４）の何れかを用いて暗号鍵Ｋcoを決定したならば、次に、手順Ｒ５として、光ディスク記録再生装置１００は、光ディスク１２に記録するデータを当該暗号鍵Ｋcoで暗号化し、その暗号化されたデータＥnc（Kco，data）を光ディスク１２に記録する。

【００６０】

また、上記暗号化Ｋco、又は暗号化した暗号鍵Ｋcoを、セキュリティモジュール１３の不揮発性メモリ３４に記録する際には、レコーディングＩＤ（Recording-ID）を検索用のキーとするために一緒に記録したり、データが記録される光ディスク１２のセクタと同一のセクタに暗号化したＫcoを記録するなどして、データと暗号鍵Ｋcoの対応がとれるようにしておく。なお、この暗号鍵Ｋcoの管理、伝送と、データの暗号化には、その処理速度の観点から共通鍵暗号アルゴリズムを使用することが好適である。

【００６１】

共通鍵暗号アルゴリズムは、暗号化とその復号の処理に同一の暗号鍵を用いる暗号アルゴリズムであり、ＦＩＰＳ４６－２で米国の標準に指定されているいわゆるＤＥＳ（Data Encryption Standard）をその例として挙げることできる。

【００６２】

特に、上記暗号鍵決定方法（４）の場合には、光ディスク記録再生装置１００が暗号鍵Ｋcoを決められるため、光ディスク記録再生装置１００は予めデータを暗号化しておくことが可能になる。

【００６３】

当該第１の実施の形態では、以上の手順により、データを光ディスク１２に記録する。

【００６４】

次に、図７には、上記図６に示した第１の実施の形態の光ディスク記録再生装置１００が光ディスク情報記録媒体１０にデータを記録するまでの手順の詳細を

示す。なお、この図７では、光ディスク記録再生装置１００に係る各情報について「Ｂ」の文字を付し、光ディスク情報記録媒体１０のセキュリティモジュール１３に係る各情報について「Ａ」の文字を付している。また、図６で説明したのと同様に、光ディスク記録再生装置１００とセキュリティモジュール１３は、センタＴＣから与えられたＩＤ（セキュリティモジュール１３のＩＤ$_A$，光ディスク記録再生装置１００のＩＤ$_B$）、公開鍵暗号系の秘密鍵、公開鍵、公開鍵証明書、及びリボケーションリストを、それぞれ対応する不揮発性メモリ１１０，３４に格納している。

【００６５】

図７において、先ず、光ディスク記録再生装置１００は、手順Ｒ１１として、前記乱数発生部１０７にて６４ビットの乱数R_Bを生成し、この乱数R_Bを記録コマンド（記録開始コマンド）と共にセキュリティモジュール１３に送る。

【００６６】

上記記録コマンドと乱数R_Bを受け取ったセキュリティモジュール１３は、手順Ｒ１２として、前記乱数発生部３３にて６４ビットの乱数R_Aを発生すると共に、当該セキュリティモジュール１３から外部に出力されることのない秘密の所定値或いは乱数のK_A（$0<K_A<r$）を生成し、前記ＥＣ－ＤＨアルゴリズムの第１段階（ステップ１）においてpahese 1 value V_Aの値を計算（$V_A=K_A \cdot G$）により求める。なお、$V_A=K_A \cdot G$は、いわゆる楕円関数を用いた暗号技術における楕円曲線上の演算であり、Ｇは楕円曲線上のある点を表し、システムにおいて共通に設定されている値である。また、ｒは楕円関数の位数である。更に、セキュリティモジュール１３は、前記ＥＣ－ＤＳＡの署名アルゴリズムを用いて、上記乱数R_A、乱数R_B、値V_A、リボケーションリストのバージョンナンバー$RevV_A$からなるビット列$R_A||R_B||V_A||RevV_A$にデジタル署名の関数Signを用いたデジタル署名を行い$Sig_A=Sign\ (PriKey_A,\ R_A||R_B||V_A||RevV_A)$を得る。なお、$PriKey_A$はセキュリティモジュール１３のプライベート鍵であり、「||」はビットの連結を表している。セキュリティモジュール１３は、これらR_A，R_B，V_A，$RevV_A$，Sig_Aに証明書$Cert_A$を付け、光ディスク記録再生装置１００に送る。なお、セキュリティモジュール１３がリボケーションリストを持

たない場合或いは使用しない場合は、当該バージョンナンバーとして０を用いる。

【００６７】

上記セキュリティモジュール１３から$Cert_A$, R_A, R_B, V_A, $RevV_A$, Sig_Aを受け取ると、光ディスク記録再生装置１００は、ＥＣ－ＤＳＡの証明アルゴリズムを用いて、セキュリティモジュール１３の証明書$Cert_A$、デジタル署名Sig_A、ID_Aの検証（チェック）を行う。

【００６８】

すなわち、光ディスク記録再生装置１００は、先ず、セキュリティモジュール１３の証明書$Cert_A$の検証を行い、例えば当該検証をパスできないときには、そのセキュリティモジュール１３を備えた光ディスク情報記録媒体１０を不正な媒体とみなして当該プロトコルを終了する。

【００６９】

一方、セキュリティモジュール１３の証明書$Cert_A$の検証において正当であると判定された場合、光ディスク記録再生装置１００は、上記証明書$Cert_A$からパブリック鍵$PubKey_A$を手に入れる。次に、光ディスク記録再生装置１００は、セキュリティモジュール１３から返送されてきた乱数R_Bと、当該光ディスク記録再生装置１００が手順Ｒ１１で生成した乱数R_Bとが等しく、さらに上記デジタル署名Sig_Aが正当であると判定されたときには、次の処理に進み、そうでない場合にはセキュリティモジュール１３を備えた光ディスク情報記録媒体１０が不正な媒体であると判断して当該プロトコルを終了する。

【００７０】

上述のように、セキュリティモジュール１３から返送された乱数R_Bが先に生成したものと等しく、且つデジタル署名Sig_Aが正当であると判定されたとき、光ディスク記録再生装置１００は、自己の不揮発性メモリ１１０に格納しているリボケーションリストを用い、セキュリティモジュール１３を備えた光ディスク情報記録媒体１０のID_Aが当該リボケーションリストに掲載されていないことを検証する。この検証の結果、セキュリティモジュール１３を備えた光ディスク情報記録媒体１０のID_Aがリボケーションリストに掲載されている場合には、

当該セキュリティモジュール１３を備えた光ディスク情報記録媒体１０は不正な媒体であると判定し、当該プロトコルを終了する。

【００７１】

一方、セキュリティモジュール１３を備えた光ディスク情報記録媒体１０のID_Aが当該リボケーションリストに掲載されておらず、その光ディスク情報記録媒体１０が正当であると判断した場合、光ディスク記録再生装置１００は、手順Ｒ１３として、当該装置１００から外部に出力されることのない秘密の所定値或いは乱数のK_B（$0<K_B<r$）を生成し、前記ＥＣ－ＤＨアルゴリズムの第１段階（ステップ１）においてpahese 1 value V_B値を計算（$V_B=K_B \cdot G$）により求める。更に、光ディスク記録再生装置１００は、前記ＥＣ－ＤＳＡの署名アルゴリズムを用いて、上記乱数R_B、乱数R_A、値V_B、当該装置１００が持つリボケーションリストのバージョンナンバー$RevV_B$からなるビット列$R_B||R_A||V_B||RevV_B$にデジタル署名の関数Signを用いたデジタル署名を行い$Sig_B=Sign(PriKey_B, R_B||R_A||V_B||RevV_B)$を得る。なお、$PriKey_B$は光ディスク記録再生装置１００のプライベート鍵である。光ディスク記録再生装置１００は、これらR_B, R_A, V_B, $RevV_B$, Sig_Bに証明書$Cert_B$を付け、セキュリティモジュール１３に送る。なお、光ディスク記録再生装置１００がリボケーションリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして０を用いる。

【００７２】

上記光ディスク記録再生装置１００から$Cert_B$, R_B, R_A, V_B, $RevV_B$, Sig_Bを受け取ると、セキュリティモジュール１３は、ＥＣ－ＤＳＡの証明アルゴリズムを用いて、光ディスク記録再生装置１００の証明書$Cert_B$、デジタル署名Sig_B、ID_Bの検証（チェック）を行う。

【００７３】

すなわち、セキュリティモジュール１３は、先ず、光ディスク記録再生装置１００の証明書$Cert_B$の検証を行い、例えば当該検証をパスできないときには、その光ディスク記録再生装置１００を不正な装置とみなして当該プロトコルを終了する。

【００７４】

一方、光ディスク記録再生装置１００の証明書$Cert_B$の検証において正当であると判定された場合、セキュリティモジュール１３は、上記証明書$Cert_B$からパブリック鍵$PubKey_B$を手に入れる。次に、セキュリティモジュール１３は、光ディスク記録再生装置１００から返送されてきた乱数R_Aと、当該セキュリティモジュール１３が手順Ｒ１２で生成した乱数R_Aとが等しく、さらに上記デジタル署名Sig_Bが正当であると判定されたときには、次の処理に進み、そうでない場合には光ディスク記録再生装置１００が不正な装置であると判断して当該プロトコルを終了する。

【００７５】

上述のように、光ディスク記録再生装置１００から返送された乱数R_Aと先に生成したものとが等しく、且つデジタル署名Sig_Bが正当であると判定されたとき、セキュリティモジュール１３は、自己の不揮発性メモリ３４に格納しているリボケーションリストを用い、光ディスク記録再生装置１００のID_Bが当該リボケーションリストに掲載されていないことを検証する。この検証の結果、光ディスク記録再生装置１００のID_Bがリボケーションリストに掲載されている場合には、当該光ディスク記録再生装置１００は不正な装置であると判定し、当該プロトコルを終了する。

【００７６】

一方、光ディスク記録再生装置１００のID_Bが当該リボケーションリストに掲載されておらず、その光ディスク記録再生装置１００が正当であると判断した場合、すなわち、セキュリティモジュール１３と光ディスク記録再生装置１００の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール１３では$K_A \cdot V_B$の計算を行い、また、光ディスク記録再生装置１００では$K_B \cdot V_A$の計算を行い、さらにそれらのｘ座標の下位ｚビットをセッション鍵Ｋseとしてこれらセキュリティモジュール１３と光ディスク記録再生装置１００が共有する。

【００７７】

次に、セキュリティモジュール１３と光ディスク記録再生装置１００は、それ

ぞれ相手方が持っているリボケーションリストのバージョンナンバーのチェックを行い、自己の保持しているバージョンよりも新しい場合、手順Ｒ１４又はＲ１５として、その新しいバージョンのリボケーションリストを相手方に送る。すなわち、セキュリティモジュール１３では、光ディスク記録再生装置１００が保持しているリボケーションリストのバージョンナンバー$RevV_B$が、自己のリボケーションリストのバージョンナンバ$RevV_A$よりも新しいか否かチェックし、$RevV_A$が$RevV_B$よりも新しいとき、手順Ｒ１５として、自己の保持しているリボケーションリストを光ディスク記録再生装置１００に送る。一方、光ディスク記録再生装置１００では、セキュリティモジュール１３が保持しているリボケーションリストのバージョンナンバー$RevV_A$が、自己のリボケーションリストのバージョンナンバ$RevV_B$よりも新しいか否かチェックし、$RevV_B$が$RevV_A$よりも新しいとき、手順Ｒ１４として、自己の保持しているリボケーションリストをセキュリティモジュール１３に送る。

【００７８】

上述のように、相手方から新しいバージョンナンバーのリボケーションリストが送られてきた方は、当該リボケーションリスト内に含まれるセンタＴＣの署名ＴＣSigを検証し、当該署名ＴＣSigが正しい場合、そのリボケーションリストを用いて自己が保持している古いリボケーションリストを更新（リストのアップデート）する。一方、署名ＴＣSigが正しくない場合は、当該プロトコルを終了する。

【００７９】

その後、光ディスク記録再生装置１００は、手順Ｒ１６として、光ディスク１２に記録するコンテンツデータを暗号化するための暗号鍵（コンテンツ鍵）Ｋcoを定め、この暗号鍵Ｋcoをセッション鍵Ｋseにて暗号化した値Ｅnc（Kse, Kco）をセキュリティモジュール１３に送信する。

【００８０】

セキュリティモジュール１３は、手順Ｒ１７として、上記光ディスク記録再生装置１００から送信されてきた値Ｅnc（Kse, Kco）をセッション鍵Ｋseを用いて復号することにより、暗号鍵Ｋcoを復元し、さらに、この暗号鍵Ｋcoを自己が持

つストレージ鍵Ｋstにて暗号化した値Ｅnc（Kst，Kco）を光ディスク記録再生装置１００に送信する。

【００８１】

セキュリティモジュール１３から上記値Ｅnc（Kst，Kco）を受け取ると、光ディスク記録再生装置１００は、手順Ｒ１８として、上記暗号鍵Ｋcoを用いて暗号化したコンテンツデータを光ディスク情報記録媒体１０の光ディスク１２に記録すると共に、上記暗号鍵Ｋcoをストレージ鍵Ｋstにて暗号化した値Ｅnc（Kst，Kco）も上記光ディスク情報記録媒体１０の光ディスク１２に記録する。

【００８２】

なお、上記リボケーションリストの伝送は、上記コンテンツデータの伝送の合間、または終了後に行ってもよい。

【００８３】

上記図７の例では、セキュリティモジュール１３と光ディスク記録再生装置１００において、手順Ｒ１２，Ｒ１３にように、自己が保持しているリボケーションリスト内にそれぞれ相手方のＩＤが掲載されているか否かの検証を行った後、手順Ｒ１４，Ｒ１５にてリボケーションリストのバージョンナンバーの新旧をチェックし、新しいバージョンのリボケーションリストで古いバージョンのリボケーションリストを更新する例を挙げたが、以下に説明するように、先にリボケーションリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のリボケーションリストを用いて相手方のＩＤが掲載されているか否かを検証するようにしてもよい。この場合、必ず新しいバージョンのリボケーションリストによって相手方のＩＤがチェックされるため、より確実に不正なものであるか否かを判定できる。なお、両者のリボケーションリストのバージョンナンバーが同じ場合もあり得るので、以下の説明では、バージョンナンバーが同じ場合も考慮して説明する。

【００８４】

図８には、上述したように、先にリボケーションリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のリボケーションリストを用いて相手方のＩＤを検証するようにした場合の、データ記録時の手順を示す。

【００８５】

この図８において、光ディスク記録再生装置１００は、先ず、手順Ｒ２１として、前記図７の手順Ｒ１１と同様に乱数R_Bを生成し、この乱数R_Bを記録コマンドと共にセキュリティモジュール１３に送る。

【００８６】

上記記録コマンドと乱数R_Bを受け取ったセキュリティモジュール１３は、前記図７の手順Ｒ１２と同様に、手順Ｒ２２として、乱数R_Aを発生すると共に前記所定値或いは乱数のK_Aを生成し、$V_A = K_A \cdot G$の計算を行う。また、セキュリティモジュール１３は、前記同様にビット列$R_A||R_B||V_A||RevV_A$にデジタル署名を行い$Sig_A = Sign\ (PriKey_A,\ R_A||R_B||V_A||RevV_A)$を生成し、これら$R_A$, R_B, V_A, $RevV_A$, Sig_Aに証明書$Cert_A$を付けて光ディスク記録再生装置１００に送る。

【００８７】

上記セキュリティモジュール１３から$Cert_A$, R_A, R_B, V_A, $RevV_A$, Sig_Aを受け取ると、光ディスク記録再生装置１００は、セキュリティモジュール１３の証明書$Cert_A$、デジタル署名Sig_Aの検証（チェック）を行う。

【００８８】

すなわち、光ディスク記録再生装置１００は、先ず、セキュリティモジュール１３の証明書$Cert_A$の検証を行い、例えば当該検証をパスできないときには、そのセキュリティモジュール１３を備えた光ディスク情報記録媒体１０を不正な媒体とみなして当該プロトコルを終了する。

【００８９】

一方、セキュリティモジュール１３の証明書$Cert_A$の検証において正当であると判定された場合、光ディスク記録再生装置１００は、上記証明書$Cert_A$からパブリック鍵$PubKey_A$を手に入れる。次に、光ディスク記録再生装置１００は、セキュリティモジュール１３から返送されてきた乱数R_Bと、当該光ディスク記録再生装置１００が手順Ｒ２１で生成した乱数R_Bとが等しく、さらに上記デジタル署名Sig_Aが正当であると判定されたときには、次の処理に進み、そうでない場合にはセキュリティモジュール１３を備えた光ディスク情報記録媒体１０が不

正な媒体であると判断して当該プロトコルを終了する。

【００９０】

上述のように、セキュリティモジュール１３から返送されてきた乱数R_Bと先に生成したものが等しく、且つデジタル署名Sig_Aが正当であると判定されたとき、光ディスク記録再生装置１００は、図７の手順Ｒ１３と同様に、手順Ｒ２３として、K_B（$0<K_B<r$）を生成し、$V_B=K_B \cdot G$の計算を行う。更に、光ディスク記録再生装置１００は、上記乱数R_B、乱数R_A、値V_B、リボケーションリストバージョンナンバー$RevV_B$からなるビット列$R_B||R_A||V_B||RevV_B$にデジタル署名を行って$Sig_B=Sign\ (PriKey_B,\ R_B||R_A||V_B||RevV_B)$を生成し、これら$R_B$, R_A, V_B, $RevV_B$, Sig_Bに証明書$Cert_B$を付けてセキュリティモジュール１３に送る。

【００９１】

上記光ディスク記録再生装置１００から$Cert_B$, R_B, R_A, V_B, $RevV_B$, Sig_Bを受け取ると、セキュリティモジュール１３は、光ディスク記録再生装置１００の証明書$Cert_B$、デジタル署名Sig_Bの検証を行う。

【００９２】

すなわち、セキュリティモジュール１３は、先ず、光ディスク記録再生装置１００の証明書$Cert_B$の検証を行い、例えば当該検証をパスできないときには、その光ディスク記録再生装置１００を不正な装置とみなして当該プロトコルを終了する。

【００９３】

一方、光ディスク記録再生装置１００の証明書$Cert_B$の検証において正当であると判定された場合、セキュリティモジュール１３は、上記証明書$Cert_B$からパブリック鍵$PubKey_B$を手に入れる。次に、セキュリティモジュール１３は、光ディスク記録再生装置１００から返送されてきた乱数R_Aと、当該セキュリティモジュール１３が手順Ｒ２２で生成した乱数R_Aとが等しく、さらに上記デジタル署名Sig_Bが正当であると判定されたときには、次の処理に進み、そうでない場合には光ディスク記録再生装置１００が不正な装置であると判断して当該プロトコルを終了する。

【００９４】

上述のように、セキュリティモジュール１３と光ディスク記録再生装置１００の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール１３では$K_A \cdot V_B$の計算を行い、また、光ディスク記録再生装置１００では$K_B \cdot V_A$の計算を行い、さらにそれらのｘ座標の下位ｚビットをセッション鍵Kseとしてこれらセキュリティモジュール１３と光ディスク記録再生装置１００が共有する。

【００９５】

また、セキュリティモジュール１３と光ディスク記録再生装置１００の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール１３と光ディスク記録再生装置１００は、それぞれ相手方が持っているリボケーションリストのバージョンナンバーのチェックを行う。

【００９６】

ここで、両者のバージョンナンバーが同じである場合、光ディスク記録再生装置１００とセキュリティモジュール１３は、それぞれが保持するリボケーションリストを用いて相手方のＩＤの検証を行い、互いに相手方のＩＤがリボケーションリストに掲載されていないことを検証する。すなわち、セキュリティモジュール１３では、光ディスク記録再生装置のID_Bが自己のリボケーションリストに掲載されていないことを検証し、光ディスク記録再生装置１００では、セキュリティモジュール１３のID_Aが自己のリボケーションリストに掲載されていないことを検証する。当該相互検証の結果、両者において共にリボケーションリストに掲載されていないと判定された場合には、後段の手順Ｒ２６の処理に進む。また、セキュリティモジュール１３において、光ディスク記録再生装置１００のID_Bが自己のリボケーションリストに掲載されている場合には、当該光ディスク記録再生装置１００は不正な装置であると判定し、当該プロトコルを終了する。同じく、光ディスク記録再生装置１００において、セキュリティモジュール１３のID_Aが自己のリボケーションリストに掲載されている場合には、当該セキュリティモジュール１３は不正な媒体のものであると判定し、当該プロトコルを終了する。

【００９７】

一方、セキュリティモジュール１３と光ディスク記録再生装置１００においてそれぞれ相手方が持っているリボケーションリストのバージョンナンバーのチェックを行った結果、何れか一方の保持しているバージョンよりも他方のバージョンが新しい場合、手順Ｒ２４又はＲ２５として、上記新しいバージョンのリボケーションリストを相手方に送る。この新しいバージョンのリボケーションリストを受け取った側では当該新しいバージョンのリボケーションリストを用いて、相手方のＩＤの検証を行う。すなわち、セキュリティモジュール１３と光ディスク記録再生装置１００は、それぞれが当該新しいバージョンのリボケーションリストを用いて、互いに相手方のＩＤの検証を行う。

【００９８】

すなわち例えば、セキュリティモジュール１３のリボケーションリストのバージョンが、光ディスク記録再生装置１００のものよりも新しい場合、セキュリティモジュール１３では自己が保持するリボケーションリストを用いて光ディスク記録再生装置１００のID_Bの検証を行い、その検証の結果、光ディスク記録再生装置１００がリボケーションリストに記載されていないとき、手順Ｒ２４として、自己が保持しているリボケーションリストを光ディスク記録再生装置１００に送る。当該リボケーションリストを受け取った光ディスク記録再生装置１００は、この送られてきたリボケーションリストのバージョンナンバー$RevV_A$を先に取得しているバージョンナンバーと同じかどうかチェックし、さらに、その新しいリボケーションリストを用いてセキュリティモジュール１３のID_Aの検証を行う。その検証の結果、セキュリティモジュール１３のID_Aがリボケーションリストに記載されていない場合には、上記セキュリティモジュール１３から送られてきた当該新しいバージョンのリボケーションリスト内に含まれるセンタＴＣの署名ＴＣSigを検証し、この署名ＴＣSigが正しい場合、そのリボケーションリストを用いて自己が保持している古いリボケーションリストを更新する。一方、署名ＴＣSigが正しくない場合は、当該プロトコルを終了する。

【００９９】

また例えば、光ディスク記録再生装置１００のリボケーションリストのバージ

ョンが、セキュリティモジュール１３のものよりも新しい場合、光ディスク記録再生装置１００では自己が保持するリボケーションリストを用いてセキュリティモジュール１３のＩＤ$_A$の検証を行い、その検証の結果、セキュリティモジュール１３がリボケーションリストに記載されていないとき、手順Ｒ２５として、自己が保持しているリボケーションリストをセキュリティモジュール１３に送る。当該リボケーションリストを受け取ったセキュリティモジュール１３は、この送られてきたリボケーションリストのバージョンナンバーRevV$_B$を先に取得しているバージョンナンバーと同じかどうかチェックし、さらに、その新しいリボケーションリストを用いて光ディスク記録再生装置１００のＩＤ$_B$の検証を行い、その検証の結果、光ディスク記録再生装置１００のＩＤ$_B$がリボケーションリストに記載されていないとき、上記光ディスク記録再生装置１００から送られてきた新しいバージョンのリボケーションリスト内に含まれるセンタＴＣの署名ＴＣSigを検証し、当該署名ＴＣSigが正しい場合、そのリボケーションリストを用いて自己が保持している古いリボケーションリストを更新する。一方、署名ＴＣSigが正しくない場合は、当該プロトコルを終了する。

【０１００】

その後、光ディスク記録再生装置１００は、手順Ｒ２６として、光ディスク１２に記録するコンテンツデータを暗号化するための暗号鍵Ｋcoを定め、この暗号鍵Ｋcoをセッション鍵Ｋseにて暗号化した値Ｅnc（Kse，Kco）をセキュリティモジュール１３に送信する。

【０１０１】

セキュリティモジュール１３は、手順Ｒ２７として、上記光ディスク記録再生装置１００から送信されてきた値Ｅnc（Kse，Kco）をセッション鍵Ｋseを用いて復号することにより、暗号鍵Ｋcoを復元し、さらに、この暗号鍵Ｋcoを自己が持つストレージ鍵Ｋstにて暗号化した値Ｅnc（Kst，Kco）を光ディスク記録再生装置１００に送信する。

【０１０２】

セキュリティモジュール１３から上記値Ｅnc（Kst，Kco）を受け取ると、光ディスク記録再生装置１００は、手順Ｒ２８として、上記暗号鍵Ｋcoを用いて暗号

化したコンテンツデータを光ディスク情報記録媒体１０の光ディスク１２に記録すると共に、上記暗号鍵Ｋcoをストレージ鍵Ｋstにて暗号化した値Ｅnc（Kst，Kco）も上記光ディスク情報記録媒体１０の光ディスク１２に記録する。

【０１０３】

次に、図９～図１１を用いて、上記第１の実施の形態の光ディスク記録再生装置１００が光ディスク１２からデータを再生する手順を説明する。

【０１０４】

なお、上述したように、第１の実施の形態の光ディスク記録再生装置１００は、センタＴＣから与えられたＩＤ、公開鍵暗号系の秘密鍵、公開鍵、公開鍵証明書、及びリボケーションリストを上記不揮発性メモリ１１０に格納しており、また同様に、当該第１の実施の形態の光ディスク情報記録媒体１０のセキュリティモジュール１３は、センタＴＣから与えられたＩＤ、公開鍵暗号系の秘密鍵、公開鍵、公開鍵証明書、及びリボケーションリストを上記不揮発性メモリ３４に格納している。また、光ディスク記録再生装置１００は、再生すべきデータに付与されたレコーディングＩＤ（Recording-ID）を知っているものとする。

【０１０５】

先ず、図９において、光ディスク記録再生装置１００は、手順Ｐ１として、光ディスク情報記録媒体１０のセキュリティモジュール１３に対して、これからデータの再生を行うことを示す再生コマンド（再生開始コマンド）とレコーディングＩＤとを送る。

【０１０６】

次に、手順Ｐ２として、光ディスク記録再生装置１００及び光ディスク情報記録媒体１０のセキュリティモジュール１３は、上記再生コマンドをトリガーとして、公開鍵暗号技術を用いた相互認証及び鍵共有プロトコルを実行する。

【０１０７】

このプロトコルの内容は、データの記録時に用いられるプロトコルと同様であり、それぞれ他方が持つ公開鍵と秘密鍵が正しいことの検証と、リボケーションリストに相手方のＩＤが載せられていないことの確認を互いに行い、セッション鍵Ｋseを共有し、また自分が持つリボケーションリストのバージョンナンバーを

送り合う。また、手順Ｐ３，Ｐ４として、どちらかが相対的に新しいリボケーションリストを持っていた場合には、それを他方に送り、送られた方はそれを用いて自分のリボケーションリストを更新することも同様である。

【０１０８】

次に、データを光ディスク１２から読み出す前に、このデータを暗号化したときの暗号鍵Ｋcoを光ディスク記録再生装置１００が知ることが必要になる。

【０１０９】

暗号鍵Ｋcoは、セキュリティモジュール１３が安全にその内部の不揮発性メモリ３４に格納しているか、或いはセキュリティモジュール１３が予め格納しているストレージ鍵Ｋstを用いて当該暗号鍵Ｋcoを暗号化した値Ｅnc（Kst，Kco）として光ディスク１２に記録されている。なお、ここでは、不揮発性メモリ３４に暗号鍵Ｋcoが安全に格納されているとする。

【０１１０】

前者の場合、セキュリティモジュール１３は、手順Ｐ５として、不揮発性メモリ３４に格納されている暗号鍵Ｋcoをセッション鍵Ｋseで暗号化した値Ｅnc（Kse，Kco）を、光ディスク記録再生装置１００に送る。光ディスク記録再生装置１００では。当該値Ｅnc（Kse，Kco）をセッション鍵Ｋseを用いて復号することにより暗号鍵Ｋcoを得る。

【０１１１】

一方、後者の場合、光ディスク記録再生装置１００は、先ず、光ディスク１２から上記暗号鍵Ｋcoを暗号化した値Ｅnc（Kst，Kco）を読み出し、これをセキュリティモジュール１３に送る。セキュリティモジュール１３は、ストレージ鍵Ｋstを用いてこれを復号して暗号鍵Ｋcoを得、これをセッション鍵Ｋseで暗号化した値Ｅnc（Kse，Kco）を、手順Ｐ５として光ディスク記録再生装置１００に送る。光ディスク記録再生装置１００は、当該値Ｅnc（Kse，Kco）をセッション鍵Ｋseを用いて復号することにより暗号鍵Ｋcoを得る。

【０１１２】

上述のように、光ディスク記録再生装置１００は、手順Ｐ５により、データを暗号化したときの暗号鍵Ｋcoを得ることができる。

【０１１３】

次に、手順Ｐ６として、光ディスク記録再生装置１００は、光ディスク１２から、上記暗号鍵Ｋcoを用いて暗号化されているデータＥｎｃ（Kco, data）を読み出し、先に取得した暗号鍵Ｋcoを用いてこれを復号し使用する。

【０１１４】

以上が、光ディスク１２からデータを読み出す処理の基本的な手順である。

【０１１５】

図１０には、上記図７に示した第１の実施の形態の光ディスク記録再生装置１００が光ディスク情報記録媒体１０の光ディスク１２から、上記暗号化されているデータを読み出すまでの手順の詳細を説明する。なお、この図１０では、前述の図７等と同様に、光ディスク記録再生装置１００に係る各情報について「Ｂ」の文字を付し、セキュリティモジュール１３に係る各情報について「Ａ」の文字を付している。また、図９で説明したのと同様に、光ディスク記録再生装置１００とセキュリティモジュール１３は、センタＴＣから与えられたＩＤ（セキュリティモジュール１３のＩＤ$_A$，光ディスク記録再生装置１００のＩＤ$_B$）、公開鍵暗号系の秘密鍵、公開鍵、公開鍵証明書、及びリボケーションリストを、それぞれ対応する不揮発性メモリ１１０，３４に格納している。

【０１１６】

図１０において、先ず、光ディスク記録再生装置１００は、手順Ｐ１１として、前記前記記録時と同様に、乱数発生部１０７にて６４ビットの乱数Ｒ$_B$を生成し、この乱数Ｒ$_B$を再生コマンド（再生開始コマンド）と共にセキュリティモジュール１３に送る。

【０１１７】

上記再生コマンドと乱数Ｒ$_B$を受け取ったセキュリティモジュール１３は、手順Ｐ１２として、前記記録時と同様に、乱数発生部３３にて６４ビットの乱数Ｒ$_A$を発生すると共に、前記同様の秘密の所定値或いは乱数のＫ$_A$（０＜Ｋ$_A$＜ｒ）を生成し、前記ＥＣ－ＤＨアルゴリズムの第１段階（ステップ１）においてＶ$_A$＝Ｋ$_A$・Ｇの計算を行い、更に、前記ＥＣ－ＤＳＡの署名アルゴリズムを用いて、上記乱数Ｒ$_A$、乱数Ｒ$_B$、値Ｖ$_A$、リボケーションリストのバージョンナンバー

$RevV_A$からなるビット列$R_A||R_B||V_A||RevV_A$にデジタル署名を行ったSig_A＝Sign ($PriKey_A$, $R_A||R_B||V_A||RevV_A$)を得る。セキュリティモジュール１３は、これらR_A, R_B, V_A, $RevV_A$, Sig_Aに証明書$Cert_A$を付け、光ディスク記録再生装置１００に送る。

【０１１８】

上記セキュリティモジュール１３から$Cert_A$, R_A, R_B, V_A, $RevV_A$, Sig_Aを受け取ると、光ディスク記録再生装置１００は、前述の記録時と同様に、ＥＣ－ＤＳＡの証明アルゴリズムを用いて、セキュリティモジュール１３の証明書$Cert_A$、デジタル署名Sig_A、ID_Aの検証（チェック）を行う。すなわち、光ディスク記録再生装置１００は、セキュリティモジュール１３の証明書$Cert_A$の検証を行い、当該検証をパスできないときには、そのセキュリティモジュール１３を備えた光ディスク情報記録媒体１０を不正な媒体とみなして当該プロトコルを終了し、一方、当該検証において正当であると判定された場合には、上記証明書$Cert_A$からパブリック鍵$PubKey_A$を手に入れる。

【０１１９】

次に、光ディスク記録再生装置１００は、セキュリティモジュール１３から返送されてきた乱数R_Bと上記手順Ｐ１１で生成した乱数R_Bとが等しく、且つデジタル署名Sig_Aが正当であると判定されたときには、次の処理に進み、そうでない場合にはセキュリティモジュール１３を備えた光ディスク情報記録媒体１０が不正な媒体であると判断して当該プロトコルを終了する。

【０１２０】

上記セキュリティモジュール１３から返送されてきた乱数R_Bと先に生成したものが等しく、且つデジタル署名Sig_Aが正当であると判定されたとき、前述の記録時と同様に、光ディスク記録再生装置１００は、自己が保持しているリボケーションリストを用い、セキュリティモジュール１３のID_Aが当該リボケーションリストに掲載されていないことを検証し、その検証の結果、上記ID_Aがリボケーションリストに掲載されている場合には、当該セキュリティモジュール１３を備えた光ディスク情報記録媒体１０は不正な媒体であると判定し、当該プロトコルを終了する。一方、上記ID_Aが当該リボケーションリストに掲載されて

おらず正当な媒体であると判断した場合、光ディスク記録再生装置１００は、手順Ｐ１３として、前記記録時と同様に、所定値或いは乱数のK_B（$0 < K_B < r$）を生成し、前記ＥＣ－ＤＨアルゴリズムの第１段階（ステップ１）において$V_B = K_B \cdot G$の計算を行い、更に、前記ＥＣ－ＤＳＡの署名アルゴリズムを用いて、乱数R_B、乱数R_A、値V_B、バージョンナンバー$RevV_B$からなるビット列$R_B||R_A||V_B||RevV_B$にデジタル署名を行って$Sig_B = Sign(PriKey_B, R_B||R_A||V_B||RevV_B)$を得る。光ディスク記録再生装置１００は、これら$R_B$, R_A, V_B, $RevV_B$, Sig_Bに証明書$Cert_B$を付け、セキュリティモジュール１３に送る。

【０１２１】

上記光ディスク記録再生装置１００から$Cert_B$, R_B, R_A, V_B, $RevV_B$, Sig_Bを受け取ると、セキュリティモジュール１３は、ＥＣ－ＤＳＡの証明アルゴリズムを用いて、光ディスク記録再生装置１００の証明書$Cert_B$、デジタル署名Sig_B、ID_Bの検証（チェック）を行う。すなわち、セキュリティモジュール１３は、先ず証明書$Cert_B$の検証を行い、例えば当該検証をパスできないときには、その光ディスク記録再生装置１００を不正な装置とみなして当該プロトコルを終了し、一方、上記証明書$Cert_B$の検証において正当であると判定された場合、上記証明書$Cert_B$からパブリック鍵$PubKey_B$を手に入れる。次に、セキュリティモジュール１３は、光ディスク記録再生装置１００から返送されてきた乱数R_Aと、先に手順Ｐ１２で生成した乱数R_Aとが等しく、且つデジタル署名Sig_Bが正当であると判定されたときには、次の処理に進み、そうでない場合には光ディスク記録再生装置１００が不正な装置であると判断して当該プロトコルを終了する。

【０１２２】

上述のように、光ディスク記録再生装置１００から返送されてきた乱数R_Aと先に生成したものとが等しく、且つデジタル署名Sig_Bが正当であると判定されたとき、セキュリティモジュール１３は、自己が保持するリボケーションリストに光ディスク記録再生装置１００のID_Bが記載されていないことを検証し、その検証の結果、光ディスク記録再生装置１００のID_Bがリボケーションリストに掲載されている場合には、当該光ディスク記録再生装置１００は不正な装置で

あると判定し、当該プロトコルを終了する。

【０１２３】

光ディスク記録再生装置１００のＩＤ$_B$が当該リボケーションリストに掲載されておらず、その光ディスク記録再生装置１００が正当であると判断した場合、すなわちセキュリティモジュール１３と光ディスク記録再生装置１００の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール１３では$K_A \cdot V_B$の計算を行い、また、光ディスク記録再生装置１００では$K_B \cdot V_A$の計算を行い、さらにそれらのｘ座標の下位ｚビットをセッション鍵Ｋseとしてこれらセキュリティモジュール１３と光ディスク記録再生装置１００が共有する。

【０１２４】

次に、前記記録時と同様に、セキュリティモジュール１３と光ディスク記録再生装置１００は、それぞれ相手方が持っているリボケーションリストのバージョンナンバーのチェックを行い、自己の保持しているバージョンよりも新しい場合、手順Ｐ１４又はＰ１５として、その新しいバージョンのリボケーションリストを相手方に送る。このように、相手方から新しいバージョンナンバーのリボケーションリストが送られてきた方は、当該リボケーションリスト内に含まれるセンタＴＣの署名ＴＣSigを検証し、当該署名ＴＣSigが正しい場合にのみ、そのリボケーションリストを用いて自己が保持している古いリボケーションリストを更新（リストのアップデート）する。

【０１２５】

次に、光ディスク記録再生装置１００は、暗号化されているデータを光ディスク１２から読み出す前に、このデータを暗号化したときの暗号鍵Ｋcoを取得し、当該取得した暗号鍵Ｋcoを用いて、上記光ディスク１２から読み出した暗号化されているデータを復号する。なお、図１０の例では、セキュリティモジュール１３がストレージ鍵Ｋstを用いて暗号化した値Ｅnc（Kst，Kco）が光ディスク１２に記録されているとする。この場合、光ディスク記録再生装置１００は、先ず、手順Ｐ１６として、光ディスク１２から上記ストレージ鍵Ｋstで暗号鍵Ｋcoを暗号化した値Ｅnc（Kst，Kco）を読み出し、次に手順Ｐ１７として、当該値Ｅnc（

Kst, Kco）をセキュリティモジュール１３に送る。セキュリティモジュール１３では、予め保持しているストレージ鍵Ｋstを用いてこれを復号して暗号鍵Ｋcoを得、当該暗号鍵Ｋcoをセッション鍵Ｋseで暗号化し、その値Ｅnc（Kse, Kco）を手順Ｐ１８として光ディスク記録再生装置１００に送る。光ディスク記録再生装置１００は、当該値Ｅnc（Kse, Kco）をセッション鍵Ｋseを用いて復号することで、暗号鍵Ｋcoを得る。

【０１２６】

その後、光ディスク記録再生装置１００は、手順Ｐ１９により、暗号鍵Ｋcoにて暗号化されているデータＥnc（Kco, data）を光ディスク１２から読み出し、これを先に取得した暗号鍵Ｋcoを用いて復号する。

【０１２７】

上記図１０の例では、セキュリティモジュール１３と光ディスク記録再生装置１００において、手順Ｐ１２，Ｐ１３にように、自己が保持しているリボケーションリスト内にそれぞれ相手方のＩＤが掲載されているか否かの検証を行った後、手順Ｐ１４，Ｐ１５にてリボケーションリストのバージョンナンバーの新旧をチェックし、新しいバージョンのリボケーションリストで古いバージョンのリボケーションリストを更新する例を挙げたが、当該再生の場合も前述した記録の場合と同様に、先にリボケーションリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のリボケーションリストを用いて相手方のＩＤが掲載されているか否かを検証するようにしてもよい。この場合、必ず新しいバージョンのリボケーションリストによって相手方のＩＤがチェックされるため、より確実に不正なものであるか否かを判定できる。なお、この再生の例の場合も、前述の図８の例と同様に、両者のリボケーションリストのバージョンナンバーが同じ場合もあり得るので、以下の説明では、バージョンナンバーが同じ場合も考慮して説明する。

【０１２８】

図１１には、光ディスク１２からのデータ再生時において、上述したように、先にリボケーションリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のリボケーションリストを用いて相手方のＩＤを検証するようにし

た場合の手順を示す。

【０１２９】

この図１１において、光ディスク記録再生装置１００は、先ず、手順Ｐ２１として、前記図１０の手順Ｐ１１と同様に乱数R_Bを生成し、この乱数R_Bを再生コマンドと共にセキュリティモジュール１３に送る。

【０１３０】

上記再生コマンドと乱数R_Bを受け取ったセキュリティモジュール１３は、前記図１０の手順Ｐ１２と同様に、手順Ｐ２２として、乱数R_Aと前記所定値或いは乱数のK_Aを生成し、$V_A=K_A \cdot G$の計算を行い、更に前記同様にビット列$R_A||R_B||V_A||RevV_A$にデジタル署名を行って$Sig_A=Sign\ (PriKey_A,\ R_A||R_B||V_A||RevV_A)$を生成し、これらに証明書$Cert_A$を付けて光ディスク記録再生装置１００に送る。

【０１３１】

上記セキュリティモジュール１３から$Cert_A$, R_A, R_B, V_A, $RevV_A$, Sig_Aを受け取ると、光ディスク記録再生装置１００は、セキュリティモジュール１３の証明書$Cert_A$とデジタル署名Sig_Aの検証を行う。すなわち、光ディスク記録再生装置１００は、上記証明書$Cert_A$の検証を行い、当該証明書$Cert_A$の検証において正当であると判定された場合に、上記証明書$Cert_A$からパブリック鍵$PubKey_A$を手に入れ、次に、セキュリティモジュール１３から返送されてきた乱数R_Bと手順Ｐ２１で生成した乱数R_Bとが等しく、且つデジタル署名Sig_Aが正当であると判定されたときのみ次の処理に進む。

【０１３２】

上述のように正当であると判定されたとき、光ディスク記録再生装置１００は、図１０の手順Ｐ１３と同様に、手順Ｐ２３として、K_B（$0<K_B<r$）を生成し、$V_B=K_B \cdot G$の計算を行い、更に、乱数R_B、乱数R_A、値V_B、バージョンナンバー$RevV_B$からなるビット列$R_B||R_A||V_B||RevV_B$にデジタル署名を行って$Sig_B=Sign\ (PriKey_B,\ R_B||R_A||V_B||RevV_B)$を生成し、これら$R_B$, R_A, V_B, $RevV_B$, Sig_Bに証明書$Cert_B$を付けてセキュリティモジュール１３に送る。

【０１３３】

上記光ディスク記録再生装置１００から$Cert_B$, R_B, R_A, V_B, $RevV_B$, Sig_Bを受け取ると、セキュリティモジュール１３は、光ディスク記録再生装置１００の証明書$Cert_B$、デジタル署名Sig_Bの検証を行う。セキュリティモジュール１３は、上記証明書$Cert_B$の検証の結果、正当であると判定された場合、上記証明書$Cert_B$からパブリック鍵$PubKey_B$を手に入れ、次に、光ディスク記録再生装置１００から返送されてきた乱数R_Aと前記手順Ｐ２２で生成した乱数R_Aとが等しく、且つデジタル署名Sig_Bが正当であると判定されたとき、次の処理に進む。

【０１３４】

上述のように、セキュリティモジュール１３と光ディスク記録再生装置１００の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール１３では$K_A \cdot V_B$の計算を行い、光ディスク記録再生装置１００では$K_B \cdot V_A$の計算を行い、さらにそれらのｘ座標の下位ｚビットをセッション鍵Ｋseとしてこれらセキュリティモジュール１３と光ディスク記録再生装置１００が共有する。また、セキュリティモジュール１３と光ディスク記録再生装置１００の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール１３と光ディスク記録再生装置１００は、それぞれ相手方が持っているリボケーションリストのバージョンナンバーのチェックを行う。

【０１３５】

ここで、両者のバージョンナンバーが同じである場合、光ディスク記録再生装置１００とセキュリティモジュール１３は、それぞれが保持するリボケーションリストを用いて相手方のＩＤの検証を行い、互いに相手方のＩＤがリボケーションリストに掲載されていないことを検証する。

【０１３６】

一方、セキュリティモジュール１３と光ディスク記録再生装置１００においてそれぞれ相手方が持っているリボケーションリストのバージョンナンバーのチェックを行った結果、何れか一方の保持しているバージョンよりも他方のバージョンが新しい場合、手順Ｐ２４又はＰ２５として、上記新しいバージョンのリボケ

ーションリストを相手方に送り、この新しいバージョンのリボケーションリストを受け取った側では当該新しいバージョンのリボケーションリストを用いた相手方のＩＤ検証を行うと共に、古いバージョンのリボケーションリストを更新する。

【０１３７】

その後、光ディスク記録再生装置１００は、手順Ｐ２６として、光ディスク１２から上記ストレージ鍵Ｋstで暗号鍵Ｋcoを暗号化した値Ｅnc（Kst，Kco）を読み出し、次に手順Ｐ２７として、当該値Ｅnc（Kst，Kco）をセキュリティモジュール１３に送る。セキュリティモジュール１３において、ストレージ鍵Ｋstにより復号され、更にセッション鍵Ｋseで暗号鍵Ｋcoを暗号化した値Ｅnc（Kse，Kco）は、手順Ｐ２８として光ディスク記録再生装置１００に送られ、光ディスク記録再生装置１００では、当該値Ｅnc（Kse，Kco）をセッション鍵Ｋseを用いて復号することで、暗号鍵Ｋcoを得る。その後、光ディスク記録再生装置１００は、手順Ｐ２９により、光ディスクから、データＥnc（Kco，data）を読み出し、先に取得した暗号鍵Ｋcoを用いて、その復号を行う。

【０１３８】

次に、本発明の第２の実施の形態について説明する。

【０１３９】

本発明の第２の実施の形態では、情報記録媒体として、メモリ情報記録媒体を用いる。

【０１４０】

図１２には、本実施の形態のメモリ情報記録媒体２０の構成例を示す。

【０１４１】

このメモリ情報記録媒体２０は、カートリッジ２１内に、データを記録するための電気的に消去可能な大容量不揮発性メモリ（具体的には例えばフラッシュＲＯＭやＥＥＰＲＯＭ、磁気抵抗効果を用いたＭＲＡＭ（Magnetic Random Access Memory）など）からなるメモリ部２２と、セキュリティモジュール２３を備えている。

【０１４２】

上記セキュリティモジュール２３は、図１３に示すように、主要構成要素として、外部インターフェース部４１、演算部４２、乱数発生部４３、不揮発性メモリ４４、制御部４５、記録媒体インターフェース部４６を備えている。

【０１４３】

すなわち、このセキュリティモジュール２３は、図２に示したセキュリティモジュール１３と略々同じ構成及び機能を有するが、当該セキュリティモジュール２３の場合、外部とのインターフェース手段として外部インターフェース部４１を備えている。また、このセキュリティモジュール２３は、カートリッジ２１内のメモリ部２２との間のインターフェースをとるための記録媒体インターフェース（例えばフラッシュＲＯＭインターフェースなど）４６を備えており、したがって、前記メモリ部２２への情報の記録（書き込み）、再生（読み出し）は、当該セキュリティモジュール２３を介して行われる。

【０１４４】

このセキュリティモジュール２３内部の不揮発性メモリ４４は、秘密性の必要な情報や耐改ざん性が必要な情報など、重要な情報を格納するのに用いられるが、もしこのメモリ４４の容量が十分でない場合には、セキュリティモジュール２３外の、一般データを記録するための大容量のメモリ部２２にこれらの重要な情報を記録することもできる。この場合、秘密性の必要な情報については、セキュリティモジュール２３内の不揮発性メモリ４４に安全に格納してあるストレージ鍵Kstにより暗号化するなどの方法を用いて保護し、耐改ざん性の必要な情報については、重要な情報を記録するメモリ部２２のブロックのいわゆるＩＣＶ（Integrity Check Value）を計算し、セキュリティモジュール２３内の不揮発性メモリ４４に格納しておき、セキュリティモジュール２３外のメモリ部２２から情報を読み出す際に再びそのブロックのＩＣＶを計算し、格納してある値と比較することによって情報が改ざんされていないことを確認するなどの保護策をとる。

【０１４５】

ＩＣＶは、あるデータの完全性（Integrity、改ざんされていないこと）を保証するために、データと、何らかの秘密値（この場合、例えばセキュリティモジ

ュール２３のストレージ鍵Ｋst）とを入力とし、予め定められたアルゴリズムによって計算される値である。これによれば、上記の秘密値を知っているものしか任意のデータに対するＩＣＶを計算することが事実上できないため、例えばデータが変更されたような場合には、読み出し時に同様の方法で計算されるＩＣＶと記録時に計算されてセキュリティモジュール２３内に格納されている値とが異なることになるため、上記データが変更された事実をセキュリティモジュール２３は知ることができるようになる。

【０１４６】

なお、ＩＣＶを計算するアルゴリズムとしては、公開鍵暗号技術を用いたデジタル署名アルゴリズムや、共通鍵暗号技術を用いたＭＡＣ（Message Authentication Code）作成アルゴリズム、鍵つきハッシュ関数を用いるアルゴリズムなどがある。ＩＣＶについては、例えば、Menezesの他、「Handbook of applied cryptography」、CRC、ISBN 0－8493-8523-7、pp. 352－368に詳しい解説がある。

【０１４７】

図１４は、上記第２の実施の形態のメモリ情報記録媒体２０に対してデータ等の記録／再生（書き込み／読み出し）を行うメモリ記録再生装置２００の構成例を表している。

【０１４８】

この図１４に示したメモリ記録再生装置２００は、主要構成要素として、入出力端子２０１、制御部２０５、入力部２０６、乱数発生部２０７、インターフェース部２０８、演算部２０９、不揮発性メモリ２１０などを備えて成る。

【０１４９】

このメモリ記録再生装置２００は、図３に示した光ディスク記録再生装置１００とその構成が略々同じであるが、図３における光ディスク１２用の構成要素であるスピンドルモータ１０１、光学ヘッド１０２やサーボ回路１０３などは存在せず、その代わりに、セキュリティモジュール２３を介してメモリ情報記録媒体２０への記録／再生のためのインターフェースが設けられる。なお、図１４の例では、セキュリティモジュール２３にアクセスするためのインターフェース部２０８が、上記メモリ情報記録媒体２０への記録／再生のためのインターフェース

の機能を兼用している。また、この図１４の場合、メモリ情報記録媒体２０の入出力端子２４と、メモリ記録再生装置２００の入出力端子２０１が電気的に接続される。

【０１５０】

記録／再生回路２０４は、制御部２０５により動作モードが切り換えられる暗号化部２０４Ａと復号部２０４Ｂを有する。暗号化部２０４Ａは、記録モード時に、外部から記録信号の供給を受けると、その記録信号を暗号化し、インターフェース部２０８に供給して、メモリ情報記録媒体２０のメモリ部２２に記録させる。復号部２０４Ｂは、再生モード時に、メモリ情報記録媒体２０のメモリ部２２から再生されたデータを復号し、外部に再生信号として出力する。

【０１５１】

また、入力部２０６は、前記図３の入力部１０６と同様に、ボタン、スイッチ、リモートコントローラなどにより構成され、ユーザにより入力操作がなされたとき、その入力操作に対応する信号を出力する。制御部２０５は、記憶されている所定のコンピュータプログラムに従って、装置全体を制御する。乱数発生部２０７は、制御部２０５の制御により、所定の乱数を発生する。インターフェース２０８部は、メモリ情報記録媒体２０の入出力端子２４及びメモリ記録再生装置２００の入出力端子２０１を介して、メモリ情報記録媒体２０のセキュリティモジュール２３との間でデータの授受を行う。

【０１５２】

さらに、この第２の実施の形態のメモリ記録再生装置２００は、演算部２０９と不揮発性メモリ２１０をも備えている。これら演算部２０９及び不揮発性メモリ２１０は、前記図３の構成の演算部１０９及び不揮発性メモリ１１０と同様の機能を有している。

【０１５３】

次に、図１５から図１８を用いて、第２の実施の形態のメモリ記録再生装置２００がメモリ情報記録媒体２０にデータを記録する手順を説明する。

【０１５４】

なお、当該第２の実施の形態のメモリ記録再生装置２００は、センタＴＣから

与えられたＩＤ、公開鍵暗号系の秘密鍵、公開鍵、公開鍵証明書、及びリボケーションリストを上記不揮発性メモリ２１０に格納しており、また同様に、当該第２の実施の形態のメモリ情報記録媒体２０のセキュリティモジュール２３は、センタＴＣから与えられたＩＤ、公開鍵暗号系の秘密鍵、公開鍵、公開鍵証明書、及びリボケーションリストを上記不揮発性メモリ４４に格納している。

【０１５５】

先ず、図１５において、メモリ記録再生装置２００は、手順Ｒ３１として、メモリ情報記録媒体２０のセキュリティモジュール２３に対して、これからデータの記録を行うことを示す記録コマンド（記録開始コマンド）と、１回１回の記録を識別するために個別に割り当てるレコーディングＩＤ（Recording-ID）とを送る。

【０１５６】

次に、手順Ｒ３２として、メモリ記録再生装置２００及びメモリ情報記録媒体２０のセキュリティモジュール２３は、上記記録コマンドをトリガーとして、公開鍵暗号技術を用いた相互認証及び鍵共有プロトコルを実行する。このプロトコルの内容は、前述した第１の実施の形態におけるデータの記録時に用いられるプロトコルと同様であり、それぞれ他方が持つ公開鍵と秘密鍵が正しいことの検証と、リボケーションリストに相手方のＩＤが載せられていないことの確認を互いに行い、セッション鍵Ｋseを共有し、また自分が持つリボケーションリストのバージョンナンバーを送り合う。

【０１５７】

また、前記図６の手順Ｒ３，Ｒ４と同様に、図１５の手順Ｐ３３，Ｐ３４として、どちらかが相対的に新しいリボケーションリストを持っていた場合には、それを他方に送り、送られた方はそれを用いて自分のリボケーションリストを更新することも同様である。すなわち、手順Ｒ３３には、セキュリティモジュール２３上のリボケーションリストのバージョンが、記録再生装置２００上のリボケーションリストのバージョンよりも新しい場合におけるリボケーションリストの流れを示しており、また、手順Ｒ３４には、記録再生装置２００上のリボケーションリストのバージョンが、セキュリティモジュール２３上のリボケーションリス

トのバージョンよりも新しい場合におけるリボケーションリストの流れを示している。

【０１５８】

なお、手順Ｒ３３，Ｒ３４におけるリボケーションリストの送付は、後の手順Ｒ３５，Ｒ３６におけるデータの記録と順序が前後してもかまわない。つまり、手順Ｒ３５，Ｒ３６にてデータの記録を行った後に、手順Ｒ３３或いはＲ３４でのリボケーションリストの送付を行うようにしてもよい。

【０１５９】

ここで、当該第２の実施の形態においても前記第１の実施の形態の場合と同様に、データを暗号化する暗号鍵Ｋcoを決定するが、その決定方法としては、以下に述べる暗号鍵決定方法（１１）～（１４）のうちの一つを用いればよい。

【０１６０】

すなわち、この第２の実施の形態の場合、暗号鍵決定方法（１１）では、Ｋse＝Ｋcoとする。この時、セキュリティモジュール２３は、暗号鍵Ｋcoを安全にその内部の不揮発性メモリ４４に格納するか、セキュリティモジュール２３が予め格納しているストレージ鍵Ｋstを用いて当該暗号鍵Ｋcoを暗号化した値Ｅnc（Kst，Kco）を、当該セキュリティモジュール２３外のメモリ部２２に格納する。

【０１６１】

暗号鍵決定方法（１２）では、セキュリティモジュール２３が予め格納しているストレージ鍵Ｋstを暗号鍵Ｋcoとする。この場合、セキュリティモジュール２３がストレージ鍵Ｋstを上記セッション鍵Ｋseで暗号化してメモリ記録再生装置２００に送る。

【０１６２】

暗号鍵決定方法（１３）では、セキュリティモジュール２３がそのデータ用の暗号鍵Ｋcoを乱数発生器などを用いて新たに発生させる。この場合、セキュリティモジュール２３が当該暗号鍵Ｋcoを上記セッション鍵Ｋseで暗号化してメモリ記録再生装置２００に送る。また、セキュリティモジュール２３は、暗号鍵Ｋcoを安全にその内部の不揮発性メモリ４４に格納するか、セキュリティモジュール２３が予め格納しているストレージ鍵Ｋstを用いて上記暗号鍵Ｋcoを暗号化した

値Ｅnc（Kst，Kco）を上記メモリ部２２に格納する。

【０１６３】

暗号鍵決定方法（１４）では、メモリ記録再生装置２００がそのデータ用の暗号鍵Ｋcoを乱数発生器などを用いて新たに発生させる。この場合、メモリ記録再生装置２００が暗号鍵Ｋcoをセッション鍵Ｋseで暗号化してセキュリティモジュール２３に送る。セキュリティモジュール２３は暗号鍵Ｋcoを安全にその内部の不揮発性メモリ４４に格納するか、セキュリティモジュール２３が予め格納しているストレージ鍵Ｋstを用いて暗号鍵Ｋcoを暗号化した値Ｅnc（Kst，Kco）を上記メモリ部２２に格納する。

【０１６４】

~~上述した暗号鍵決定方法（１１）～（１４）の何れかを用いて暗号鍵Ｋcoを決~~定したならば、次に、手順Ｒ３５として、メモリ記録再生装置２００は、メモリ情報記録媒体２０のメモリ部２２に記録するデータを当該暗号鍵Ｋcoで暗号化し、その暗号化されたデータＥnc（Kco，data）をセキュリティモジュール２３に伝送する。

【０１６５】

この時のセキュリティモジュール２３は、手順Ｒ３６として、当該暗号化されたデータＥnc（Kco，data）を、上記大容量のメモリ部２２に格納する。

【０１６６】

また、上記暗号化Ｋco、又は暗号化した暗号鍵Ｋcoを、セキュリティモジュール２３の不揮発性メモリ４４、又はメモリ部２２に記録する際には、レコーディングＩＤを検索用のキーとするために一緒に記録したり、データが記録されるメモリ部２２のセクタと同一のセクタに、上記暗号化した暗号鍵Ｋcoを記録するなどして、データと暗号鍵Ｋcoとの対応がとれるようにしておく。なお、この暗号鍵Ｋcoの管理、伝送と、データの暗号化には、その処理速度の観点から共通鍵暗号アルゴリズムを使用することが好適である。

【０１６７】

また特に、上記暗号鍵決定方法（１４）の場合には、メモリ記録再生装置２００が暗号鍵Ｋcoを決められるため、メモリ記録再生装置２００は予めデータを暗

号化しておくことが可能になる。

【０１６８】

当該第２の実施の形態では、以上の手順により、データをメモリ情報記録媒体２０の大容量メモリ部２２に記録する。

【０１６９】

次に、図１６には、上記図１５に示した第２の実施の形態のメモリ記録再生装置２００がメモリ情報記録媒体２０にデータを記録するまでの手順の詳細を示す。なお、この図１６では、メモリ記録再生装置２００に係る各情報について「Ｂ」の文字を付し、メモリ情報記録媒体２０のセキュリティモジュール２３に係る各情報について「Ａ」の文字を付している。また、図１５で説明したのと同様に、メモリ記録再生装置２００とセキュリティモジュール２３は、センタＴＣから与えられたＩＤ（セキュリティモジュール２３のＩＤ$_A$，メモリ記録再生装置２００のＩＤ$_B$）、公開鍵暗号系の秘密鍵、公開鍵、公開鍵証明書、及びリボケーションリストを、それぞれ対応する不揮発性メモリ２１０，４４に格納している。

【０１７０】

図１６の手順Ｒ４１～手順Ｒ４６までは、前述した第１の実施の形態における図７の手順Ｒ１１～手順Ｒ１６までと略々同じである。

【０１７１】

すなわち、メモリ記録再生装置２００は、手順Ｒ４１として乱数Ｒ$_B$を生成して記録コマンドと共にセキュリティモジュール２３に送り、当該記録コマンドと乱数Ｒ$_B$を受け取ったセキュリティモジュール２３は、手順Ｒ４２として、乱数Ｒ$_A$とＫ$_A$を生成し、次にＶ$_A$＝Ｋ$_A$・Ｇの計算を行い、乱数Ｒ$_A$、乱数Ｒ$_B$、値Ｖ$_A$、バージョンナンバーＲｅｖＶ$_A$からなるビット列にデジタル署名を行ってＳｉｇ$_A$を得、これらＲ$_A$，Ｒ$_B$，Ｖ$_A$，ＲｅｖＶ$_A$，Ｓｉｇ$_A$と証明書Ｃｅｒｔ$_A$をメモリ記録再生装置２００に送る。なお、セキュリティモジュール２３がリボケーションリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして０を用いる。

【０１７２】

上記セキュリティモジュール２３から$Cert_A$, R_A, R_B, V_A, $RevV_A$, Sig_Aを受け取ると、メモリ記録再生装置２００は、証明書$Cert_A$の検証を行い、その検証をパスできないときには、そのセキュリティモジュール２３を備えたメモリ情報記録媒体２０を不正な媒体とみなして当該プロトコルを終了し、一方、証明書$Cert_A$の検証において正当であると判定された場合、上記証明書$Cert_A$からパブリック鍵$PubKey_A$を手に入れる。次に、メモリ記録再生装置２００は、セキュリティモジュール２３から返送されてきた乱数R_Bと、先の手順Ｒ４１で生成した乱数R_Bとが等しく、且つデジタル署名Sig_Aが正当であると判定されたときには、次の処理に進み、そうでない場合にはセキュリティモジュール２３を備えたメモリ情報記録媒体２０が不正な媒体であると判断して当該プロトコルを終了する。

【０１７３】

上記セキュリティモジュール２３から返送されてきた乱数R_Bと先に生成したものとが等しく、且つデジタル署名Sig_Aが正当であると判定されたとき、メモリ記録再生装置２００は、自己の不揮発性メモリ２１０に格納しているリボケーションリストを用い、セキュリティモジュール２３を備えたメモリ情報記録媒体２０のID_Aが当該リボケーションリストに掲載されていないことを検証し、この検証の結果、上記ID_Aがリボケーションリストに掲載されている場合には、当該セキュリティモジュール２３を備えたメモリ情報記録媒体２０は不正な媒体であると判定し、当該プロトコルを終了する。一方、上記ID_Aが当該リボケーションリストに掲載されていない場合、メモリ記録再生装置２００は、手順Ｒ４３として、K_Bを生成して$V_B=K_B \cdot G$の計算を行い、更に、上記乱数R_B、乱数R_A、値V_B、バージョンナンバー$RevV_B$からなるビット列にデジタル署名を行ってSig_Bを得る。次にメモリ記録再生装置２００は、これらR_B, R_A, V_B, $RevV_B$, Sig_Bと証明書$Cert_B$を、セキュリティモジュール２３に送る。なお、メモリ記録再生装置２００がリボケーションリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして０を用いる。

【０１７４】

上記メモリ記録再生装置２００から$Cert_B$, R_B, R_A, V_B, $RevV_B$, Sig_Bを受け取ると、セキュリティモジュール２３は、上記証明書$Cert_B$の検証を行い、当該検証をパスできないときには、そのメモリ記録再生装置２００を不正な装置とみなして当該プロトコルを終了し、一方、上記証明書$Cert_B$の検証において正当であると判定された場合は、上記証明書$Cert_B$からパブリック鍵$PubKey_B$を手に入れる。次に、セキュリティモジュール２３は、メモリ記録再生装置２００から返送されてきた乱数R_Aと先に手順Ｒ４２で生成した乱数R_Aとが等しく、且つデジタル署名Sig_Bが正当であると判定されたときには、次の処理に進み、そうでない場合にはメモリ記録再生装置２００が不正な装置であると判断して当該プロトコルを終了する。

【０１７５】

上記メモリ記録再生装置２００から返送されてきた乱数R_Aと先に生成したものとが等しく、且つデジタル署名Sig_Bが正当であると判定されたとき、セキュリティモジュール２３は、自己の不揮発性メモリ４４に格納しているリボケーションリストを用い、上記ID_Bが当該リボケーションリストに掲載されていないことを検証し、その検証の結果、上記ID_Bがリボケーションリストに掲載されている場合には、当該メモリ記録再生装置２００は不正な装置であると判定し、当該プロトコルを終了する。

【０１７６】

一方、上記ID_Bがリボケーションリストに掲載されていない場合、すなわち、セキュリティモジュール２３とメモリ記録再生装置２００の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール２３では$K_A \cdot V_B$の計算を行い、また、メモリ記録再生装置２００では$K_B \cdot V_A$の計算を行い、さらにそれらのｘ座標の下位ｚビットをセッション鍵Ｋseとしてこれらセキュリティモジュール２３とメモリ記録再生装置２００が共有する。

【０１７７】

次に、セキュリティモジュール２３とメモリ記録再生装置２００は、それぞれ相手方が持っているリボケーションリストのバージョンナンバーのチェックを行

い、自己の保持しているバージョンよりも新しい場合、手順Ｒ４４又はＲ４５として、その新しいバージョンのリボケーションリストを相手方に送る。このように、相手方から新しいバージョンナンバーのリボケーションリストが送られてきた方は、当該リボケーションリスト内に含まれるセンタＴＣの署名ＴＣSigを検証し、当該署名ＴＣSigが正しい場合、そのリボケーションリストを用いて自己が保持している古いリボケーションリストを更新し、一方で、署名ＴＣSigが正しくない場合は、当該プロトコルを終了する。

【０１７８】

その後、メモリ記録再生装置２００は、手順Ｒ４６として、メモリ情報記録媒体２０のメモリ部２２に記録するコンテンツデータを暗号化するための暗号鍵Ｋcoを定め、この暗号鍵Ｋcoをセッション鍵Ｋseにて暗号化した値Ｅnc（Kse，Kco）をセキュリティモジュール２３に送信する。

【０１７９】

この時のセキュリティモジュール２３は、手順Ｒ４７として、上記メモリ記録再生装置２００から送信されてきた値Ｅnc（Kse，Kco）をセッション鍵Ｋseを用いて復号して暗号鍵Ｋcoを復元し、さらに、この暗号鍵Ｋcoを自己のストレージ鍵Ｋstにて暗号化した値Ｅnc（Kst，Kco）をメモリ部２２に格納し、或いは暗号鍵Ｋcoを不揮発性メモリ４４に格納する。

【０１８０】

その後、メモリ記録再生装置２００は、手順Ｒ４８として、上記暗号鍵Ｋcoを用いて暗号化したコンテンツデータＥnc（Kco，data）をセキュリティモジュール２３に送る。

【０１８１】

この時のセキュリティモジュール２３は、手順Ｒ４９として、当該暗号化されているコンテンツデータＥnc（Kco，data）をメモリ部２２に格納する。

【０１８２】

なお、上記リボケーションリストの伝送は、上記コンテンツデータの伝送の合間、または終了後に行ってもよい。

【０１８３】

上記図１６の例では、セキュリティモジュール２３とメモリ記録再生装置２００において、手順Ｒ４２，Ｒ４３にように、自己が保持しているリボケーションリスト内にそれぞれ相手方のＩＤが掲載されているか否かの検証を行った後、手順Ｒ４４，Ｒ４５にてリボケーションリストのバージョンナンバーの新旧をチェックし、新しいバージョンのリボケーションリストで古いバージョンのリボケーションリストを更新する例を挙げたが、以下に説明するように、先にリボケーションリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のリボケーションリストを用いて相手方のＩＤが掲載されているか否かを検証するようにしてもよい。この場合、必ず新しいバージョンのリボケーションリストによって相手方のＩＤがチェックされるため、より確実に不正なものであるか否かを判定できる。なお、両者のリボケーションリストのバージョンナンバーが同じ場合もあり得るので、以下の説明では、バージョンナンバーが同じ場合も考慮して説明する。

【０１８４】

図１７には、第２の実施の形態において、上述のように先にリボケーションリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のリボケーションリストを用いて相手方のＩＤを検証するようにした場合の、データ記録時の手順を示す。

【０１８５】

なお、図１７の手順Ｒ５１～手順Ｒ５６までは、前述した第１の実施の形態における図８の手順Ｒ２１～手順Ｒ２６までと略々同じである。

【０１８６】

この図１７において、メモリ記録再生装置２００は、手順Ｒ５１として、乱数R_Bを記録コマンドと共にセキュリティモジュール２３に送る。上記記録コマンドと乱数R_Bを受け取ったセキュリティモジュール２３は、手順Ｒ５２として、乱数R_AとK_Aを生成し、$V_A=K_A \cdot G$の計算を行い、さらに、前記同様に乱数R_A、乱数R_B、値V_A、バージョンナンバー$RevV_A$からなるビット列にデジタル署名を行ってSig_Aを生成し、それらR_A，R_B，V_A，$RevV_A$，Sig_Aと証明書Cer

t_Aをメモリ記録再生装置２００に送る。

【０１８７】

上記セキュリティモジュール２３から$Cert_A$, R_A, R_B, V_A, $RevV_A$, Sig_Aを受け取ると、メモリ記録再生装置２００は、証明書$Cert_A$、デジタル署名Sig_Aの検証を行う。すなわち、メモリ記録再生装置２００は、証明書$Cert_A$の検証を行い、当該検証をパスできないときには、そのセキュリティモジュール２３を備えたメモリ情報記録媒体２０を不正な媒体とみなして当該プロトコルを終了し、一方で、証明書$Cert_A$の検証において正当であると判定された場合は、上記証明書$Cert_A$からパブリック鍵$PubKey_A$を手に入れる。次に、メモリ記録再生装置２００は、セキュリティモジュール２３から返送されてきた乱数R_Bと先の手順Ｒ５１で生成した乱数R_Bとが等しく、且つデジタル署名Sig_Aが正当であると判定されたときには、次の処理に進み、そうでない場合にはセキュリティモジュール２３を備えたメモリ情報記録媒体２０が不正な媒体であると判断して当該プロトコルを終了する。

【０１８８】

上記メモリ記録再生装置２００から返送されてきた乱数R_Bと先に生成したものとが等しく、且つデジタル署名Sig_Aが正当であると判定されたとき、メモリ記録再生装置２００は、手順Ｒ５３として、K_Bを生成し、$V_B=K_B \cdot G$の計算を行い、更に、上記乱数R_B、乱数R_A、値V_B、バージョンナンバー$RevV_B$からなるビット列にデジタル署名を行ってSig_Bを生成し、これらR_B, R_A, V_B, $RevV_B$, Sig_Bと証明書$Cert_B$をセキュリティモジュール２３に送る。

【０１８９】

上記メモリ記録再生装置２００から$Cert_B$, R_B, R_A, V_B, $RevV_B$, Sig_Bを受け取ると、セキュリティモジュール２３は、メモリ記録再生装置２００の証明書$Cert_B$、デジタル署名Sig_Bの検証を行う。すなわち、セキュリティモジュール２３は、先ず、証明書$Cert_B$の検証を行い、当該検証をパスできないときには、そのメモリ記録再生装置２００を不正な装置とみなして当該プロトコルを終了し、一方で、証明書$Cert_B$の検証において正当であると判定された場合には、上記証明書$Cert_B$からパブリック鍵$PubKey_B$を手に入れる。次に、セキュリティ

モジュール２３は、メモリ記録再生装置２００から返送されてきた乱数R_Aと先の手順Ｒ５２で生成した乱数R_Aとが等しく、且つデジタル署名Sig_Bが正当であると判定されたときには、次の処理に進み、そうでない場合にはメモリ記録再生装置２００が不正な装置であると判断して当該プロトコルを終了する。

【０１９０】

上述のように、セキュリティモジュール２３とメモリ記録再生装置２００の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール２３では$K_A \cdot V_B$の計算を行い、また、メモリ記録再生装置２００では$K_B \cdot V_A$の計算を行い、さらにそれらのｘ座標の下位ｚビットをセッション鍵Ｋseとしてこれらセキュリティモジュール２３とメモリ記録再生装置２００が共有する。

【０１９１】

また、セキュリティモジュール２３とメモリ記録再生装置２００の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール２３とメモリ記録再生装置２００は、それぞれ相手方が持っているリボケーションリストのバージョンナンバーのチェックを行う。

【０１９２】

ここで、両者のバージョンナンバーが同じである場合、メモリ記録再生装置２００とセキュリティモジュール２３は、それぞれが保持するリボケーションリストを用いて相手方のＩＤの検証を行い、互いに相手方のＩＤがリボケーションリストに掲載されていないことを検証する。当該相互検証の結果、両者において共にリボケーションリストに掲載されていないと判定された場合には、後段の手順Ｒ５６の処理に進む。また、セキュリティモジュール２３において、メモリ記録再生装置２００のID_Bが自己のリボケーションリストに掲載されている場合には、当該メモリ記録再生装置２００は不正な装置であると判定し、当該プロトコルを終了する。同じく、メモリ記録再生装置２００において、セキュリティモジュール２３のID_Aが自己のリボケーションリストに掲載されている場合には、当該セキュリティモジュール２３は不正な媒体のものであると判定し、当該プロトコルを終了する。

【０１９３】

一方、セキュリティモジュール２３とメモリ記録再生装置２００においてそれぞれ相手方が持っているリボケーションリストのバージョンナンバーのチェックを行った結果、何れか一方の保持しているバージョンよりも他方のバージョンが新しい場合、手順Ｒ５４又はＲ５５として、上記新しいバージョンのリボケーションリストを相手方に送り、この新しいバージョンのリボケーションリストを受け取った側では当該新しいバージョンのリボケーションリストを用いて相手方のＩＤ検証を行うと共に、古いバージョンのリボケーションリストを更新する。

【０１９４】

すなわち例えば、セキュリティモジュール２３のリボケーションリストのバージョンが、メモリ記録再生装置２００のものよりも新しい場合、セキュリティモジュール２３では自己が保持するリボケーションリストを用いてメモリ記録再生装置２００のID_Bの検証を行い、その検証の結果、メモリ記録再生装置２００がリボケーションリストに記載されていないとき、手順Ｒ５４として、自己が保持しているリボケーションリストをメモリ記録再生装置２００に送る。当該リボケーションリストを受け取ったメモリ記録再生装置２００は、当該送られてきた新しいリボケーションリストを用いてセキュリティモジュール２３のID_Aの検証を行い、その検証の結果、セキュリティモジュール２３のID_Aがリボケーションリストに記載されていないとき、上記セキュリティモジュール２３から送られてきた新しいバージョンのリボケーションリスト内に含まれるセンタＴＣの署名ＴＣSigを検証し、当該署名ＴＣSigが正しい場合、そのリボケーションリストを用いて自己が保持している古いリボケーションリストを更新する。一方、署名ＴＣSigが正しくない場合は、当該プロトコルを終了する。

【０１９５】

また、メモリ記録再生装置２００のリボケーションリストのバージョンが、セキュリティモジュール２３のものよりも新しい場合、メモリ記録再生装置２００では自己が保持するリボケーションリストを用いてセキュリティモジュール２３のID_Aの検証を行い、その検証の結果、セキュリティモジュール２３がリボケーションリストに記載されていないとき、手順Ｒ５５として、自己が保持してい

るリボケーションリストをセキュリティモジュール２３に送る。当該リボケーションリストを受け取ったセキュリティモジュール２３は、その送られてきた新しいリボケーションリストを用いてメモリ記録再生装置２００のＩＤ$_B$の検証を行い、その検証の結果、メモリ記録再生装置２００のＩＤ$_B$がリボケーションリストに記載されていないとき、上記メモリ記録再生装置２００から送られてきた新しいバージョンのリボケーションリスト内に含まれるセンタＴＣの署名ＴＣSigを検証し、当該署名ＴＣSigが正しい場合、そのリボケーションリストを用いて自己が保持している古いリボケーションリストを更新する。一方、署名ＴＣSigが正しくない場合は、当該プロトコルを終了する。

【０１９６】

~~次に、メモリ記録再生装置２００は、手順Ｒ５６として、メモリ情報記録媒体~~２０のメモリ部２２に記録するコンテンツデータを暗号化するための暗号鍵Ｋcoをセッション鍵Ｋseにて暗号化した値Ｅnc（Kse，Kco）をセキュリティモジュール２３に送信する。

【０１９７】

この時のセキュリティモジュール２３は、手順Ｒ５７として、上記メモリ記録再生装置２００から送信されてきた値Ｅnc（Kse，Kco）をセッション鍵Ｋseを用いて復号することにより、暗号鍵Ｋcoを復元し、さらに、この暗号鍵Ｋcoを自己が持つストレージ鍵Ｋstにて暗号化した値Ｅnc（Kst，Kco）をメモリ部２２或いは不揮発性メモリ４４に格納する。

【０１９８】

その後、メモリ記録再生装置２００は、手順Ｒ５８として、上記暗号鍵Ｋcoを用いて暗号化したコンテンツデータＥnc（Kco，data）をセキュリティモジュール２３に送る。

【０１９９】

この時のセキュリティモジュール２３は、手順Ｒ５９として、当該暗号化されているコンテンツデータＥnc（Kco，data）をメモリ部２２に格納する。なお、上記リボケーションリストの伝送は、上記コンテンツデータの伝送の合間、または終了後に行ってもよい。

【０２００】

次に、この第２の実施の形態において、メモリ情報記録媒体２０のメモリ部２２へのデータの記録処理については、図１８のようにすることも可能である。なお、図１８の手順Ｒ６１～Ｒ６４については、図１５の手順Ｒ３１～Ｒ３４と同じであるためその説明は省略する。

【０２０１】

この図１８の例において、メモリ記録再生装置２００は、手順Ｒ６５として、前述の認証と鍵共有プロトコルにおいてセキュリティモジュール２３と共有したセッション鍵Ｋseを用いてデータを暗号化し、当該暗号化されたデータＥnc（Kse，data）をセキュリティモジュール２３に送る。

【０２０２】

この暗号化されたデータＥnc（Kse，data）を受け取ったセキュリティモジュール２３は、手順Ｒ６６として、同じくセッション鍵Ｋseを用いてこれを復号し、平文のデータを得、次に新たに発生させた暗号鍵Ｋcoで暗号化した値Ｅnc（Kco，data）をデータ用のメモリ部２２に記録する。

【０２０３】

ここで、セキュリティモジュール２３は、暗号鍵Ｋcoを安全にその内部の不揮発性メモリ４４に格納するか、セキュリティモジュール２３が予め格納しているストレージ鍵Ｋstを用いて暗号鍵Ｋcoを暗号化した値Ｅnc（Kst，Kco）を上記大容量のメモリ部２２に格納する。このようにすると、セキュリティモジュール２３はデータの暗号鍵Ｋcoをメモリ記録再生装置２００にも教えないで済む（つまり、外部に漏らさない）ようになる。

【０２０４】

次に、図１９～図２２を用いて、上記第２の実施の形態のメモリ記録再生装置２００がメモリ情報記録媒体２０のメモリ部２２からデータを再生する手順を説明する。

【０２０５】

なお、上述したように、第２の実施の形態のメモリ記録再生装置２００は、センタＴＣから与えられたＩＤ、公開鍵暗号系の秘密鍵、公開鍵、公開鍵証明書、

及びリボケーションリストを上記不揮発性メモリ２１０に格納しており、また同様に、当該第２の実施の形態のメモリ情報記録媒体２０のセキュリティモジュール２３は、センタＴＣから与えられたＩＤ、公開鍵暗号系の秘密鍵、公開鍵、公開鍵証明書、及びリボケーションリストを上記不揮発性メモリ４４に格納している。また、メモリ記録再生装置２００は、再生すべきデータに付与されたレコーディングＩＤを知っているものとする。

【０２０６】

先ず、図１９において、メモリ記録再生装置２００は、手順Ｐ３１として、メモリ情報記録媒体２０のセキュリティモジュール２３に対して、これからデータの再生を行うことを示す再生コマンド（再生開始コマンド）と、１回１回の記録を識別するために個別に割り当てるレコーディングＩＤとを送る。

【０２０７】

次に、手順Ｐ３２として、メモリ記録再生装置２００及びメモリ情報記録媒体２０のセキュリティモジュール２３は、上記再生コマンドをトリガーとして、公開鍵暗号技術を用いた相互認証及び鍵共有プロトコルを実行する。このプロトコルの内容は、前述した第１の実施の形態におけるデータの再生時に用いられるプロトコルと同様であり、それぞれ他方が持つ公開鍵と秘密鍵が正しいことの検証と、リボケーションリストに相手方のＩＤが載せられていないことの確認を互いに行い、セッション鍵Ｋseを共有し、また自分が持つリボケーションリストのバージョンナンバーを送り合う。

【０２０８】

また、前記図１５の手順Ｒ３３，Ｒ３４と同様に、図１９の手順Ｐ３３，Ｐ３４として、どちらかが相対的に新しいリボケーションリストを持っていた場合には、それを他方に送り、送られた方はそれを用いて自分のリボケーションリストを更新することも同様である。すなわち、手順Ｐ３３には、セキュリティモジュール２３上のリボケーションリストのバージョンが、メモリ記録再生装置２００上のリボケーションリストのバージョンよりも新しい場合におけるリボケーションリストの流れを示しており、また、手順Ｐ３４には、メモリ記録再生装置２００上のリボケーションリストのバージョンが、セキュリティモジュール２３上の

リボケーションリストのバージョンよりも新しい場合におけるリボケーションリストの流れを示している。

【０２０９】

なお、手順Ｐ３３，ＲＰ４におけるリボケーションリストの送付は、後の手順Ｐ３５，Ｐ３６におけるデータの再生と順序が前後してもかまわない。つまり、手順Ｐ３５，Ｐ３６にてデータの記録を行った後に、手順Ｐ３３或いはＰ３４でのリボケーションリストの送付を行うようにしてもよい。

【０２１０】

次に、データをメモリ情報記録媒体２０のメモリ部２２から読み出す前に、このデータを暗号化したときの暗号鍵Ｋcoをメモリ記録再生装置２００が知ることが必要になる。

【０２１１】

暗号鍵Ｋcoは、セキュリティモジュール２３が安全にその内部の不揮発性メモリ４４に格納しているか、或いはセキュリティモジュール２３が予め格納しているストレージ鍵Ｋstを用いて当該暗号鍵Ｋcoを暗号化した値Ｅnc（Kst，Kco）としてメモリ部２２に記録されている。

【０２１２】

前者の場合、セキュリティモジュール２３は、不揮発性メモリ４４に格納されている暗号鍵Ｋcoをセッション鍵Ｋseで暗号化した値Ｅnc（Kse，Kco）を、メモリ記録再生装置２００に送る。メモリ記録再生装置２００では。当該値Ｅnc（Kse，Kco）をセッション鍵Ｋseを用いて復号することにより暗号鍵Ｋcoを得る。

【０２１３】

一方、後者の場合、セキュリティモジュール２３は、手順Ｐ３５として、メモリ部２２から上記ストレージ鍵Ｋstで暗号鍵Ｋcoを暗号化した値Ｅnc（Kst，Kco）を読み出し、これをストレージ鍵Ｋstを用いて復号して暗号鍵Ｋcoを得る。さらに、この暗号鍵Ｋcoをセッション鍵Ｋseで暗号化した値Ｅnc（Kse，Kco）を、手順Ｐ３６としてメモリ記録再生装置２００に送る。メモリ記録再生装置２００は、当該値Ｅnc（Kse，Kco）をセッション鍵Ｋseを用いて復号することにより暗号鍵Ｋcoを得る。

【０２１４】

上述のように、メモリ記録再生装置２００は、データを暗号化したときの暗号鍵Ｋcoを得ることができる。

【０２１５】

その後、メモリ記録再生装置２００は、上記メモリ情報記録媒体２０のメモリ部２２から、上記暗号鍵Ｋcoを用いて暗号化されているデータＥｎｃ（Kco，data）を読み出し、先に取得した暗号鍵Ｋcoを用いてこれを復号し使用する。

【０２１６】

以上が、メモリ情報記録媒体２０のメモリ部２２からデータを読み出す処理の基本的な手順である。

【０２１７】

次に、図２０には、上記第２の実施の形態のメモリ記録再生装置２００がメモリ情報記録媒体２０からデータを再生するまでの手順の詳細を示す。なお、この図２０では、メモリ記録再生装置２００に係る各情報について「Ｂ」の文字を付し、メモリ情報記録媒体２０のセキュリティモジュール２３に係る各情報について「Ａ」の文字を付している。上述同様に、メモリ記録再生装置２００とセキュリティモジュール２３は、センタＴＣから与えられたＩＤ（セキュリティモジュール２３のＩＤ$_A$，メモリ記録再生装置２００のＩＤ$_B$）、公開鍵暗号系の秘密鍵、公開鍵、公開鍵証明書、及びリボケーションリストを、それぞれ対応する不揮発性メモリ２１０，４４に格納している。

【０２１８】

図２０の手順Ｐ４１～手順Ｐ４６までは、前述した第１の実施の形態における図１０の手順Ｐ１１～手順Ｐ１６までと略々同じである。

【０２１９】

すなわち、メモリ記録再生装置２００は、手順Ｐ４１として乱数Ｒ$_B$と再生コマンドをセキュリティモジュール２３に送る。セキュリティモジュール２３は、手順Ｐ４２として、乱数Ｒ$_A$とＫ$_A$を生成し、Ｖ$_A$＝Ｋ$_A$・Ｇの計算を行い、乱数Ｒ$_A$、乱数Ｒ$_B$、値Ｖ$_A$、バージョンナンバーＲｅｖＶ$_A$からなるビット列にデジタル署名を行ってＳｉｇ$_A$を得、これらに証明書Ｃｅｒｔ$_A$を加えてメモリ記録再生装置２０

０に送る。なお、セキュリティモジュール２３がリボケーションリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして０を用いる。

【０２２０】

次に、メモリ記録再生装置２００は、証明書$Cert_A$の検証を行い、その検証をパスできないときには、そのメモリ情報記録媒体２０を不正な媒体とみなして当該プロトコルを終了し、一方、当該検証において正当であると判定された場合、上記証明書$Cert_A$からパブリック鍵$PubKey_A$を手に入れる。次に、メモリ記録再生装置２００は、セキュリティモジュール２３から返送されてきた乱数R_Bと先の手順Ｐ４１で生成した乱数R_Bとが等しく、且つデジタル署名Sig_Aが正当であると判定されたときには、次の処理に進み、そうでない場合には上記メモリ情報記録媒体２０が不正な媒体であると判断して当該プロトコルを終了する。

【０２２１】

上記セキュリティモジュール２３から返送されたきた乱数R_Bと先に生成したものとが等しく、且つデジタル署名Sig_Aが正当であると判定されたとき、メモリ記録再生装置２００は、自己が保持しているリボケーションリストを用い、上記メモリ情報記録媒体２０のID_Aが当該リボケーションリストに掲載されていないことを検証し、この検証の結果、上記ID_Aがリボケーションリストに掲載されている場合には、当該メモリ情報記録媒体２０は不正な媒体であると判定し、当該プロトコルを終了する。一方、上記ID_Aが当該リボケーションリストに掲載されていない場合、メモリ記録再生装置２００は、手順Ｐ４３として、K_Bを生成して$V_B = K_B \cdot G$の計算を行い、更に、上記乱数R_B、乱数R_A、値V_B、バージョンナンバー$RevV_B$からなるビット列にデジタル署名を行ってSig_Bを得、それらに証明書$Cert_B$を加えてセキュリティモジュール２３に送る。なお、メモリ記録再生装置２００がリボケーションリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして０を用いる。

【０２２２】

次に、セキュリティモジュール２３は、上記証明書$Cert_B$の検証を行い、当該検証をパスできないときには、そのメモリ記録再生装置２００を不正な装置とみなして当該プロトコルを終了し、一方、当該検証において正当であると判定され

た場合は、上記証明書$Cert_B$からパブリック鍵$PubKey_B$を手に入れる。次に、セキュリティモジュール２３は、メモリ記録再生装置２００から返送されてきた乱数R_Aと先に手順Ｐ４２で生成した乱数R_Aとが等しく、且つデジタル署名Sig_Bが正当であると判定されたときには、次の処理に進み、そうでない場合にはメモリ記録再生装置２００が不正な装置であると判断して当該プロトコルを終了する。

【０２２３】

上記メモリ記録再生装置２００から返送されてきた乱数R_Aと先に生成したものとが等しく、且つデジタル署名Sig_Bが正当であると判定されたとき、セキュリティモジュール２３は、自己が保持するリボケーションリストを用い、上記ID_Bが当該リボケーションリストに掲載されていないことを検証し、その検証の結果、上記ID_Bがリボケーションリストに掲載されている場合には、当該メモリ記録再生装置２００は不正な装置であると判定し、当該プロトコルを終了する。

【０２２４】

一方、上記ID_Bがリボケーションリストに掲載されていない場合、すなわち、セキュリティモジュール２３とメモリ記録再生装置２００の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール２３とメモリ記録再生装置２００は、セッション鍵Ｋseを生成して共有する。

【０２２５】

次に、セキュリティモジュール２３とメモリ記録再生装置２００は、それぞれ相手方が持っているリボケーションリストのバージョンナンバーのチェックを行い、自己の保持しているバージョンよりも新しい場合、手順Ｐ４４又はＰ４５として、その新しいバージョンのリボケーションリストを相手方に送る。このように、相手方から新しいバージョンナンバーのリボケーションリストが送られてきた方は、センタＴＣの署名ＴＣSigを検証し、当該署名ＴＣSigが正しい場合、その新しいリボケーションリストを用いた更新を行い、一方で、署名ＴＣSigが正しくない場合は、当該プロトコルを終了する。

【０２２６】

次に、暗号鍵Ｋcoを暗号化した値Ｅnc（Kst，Kco）が、例えばメモリ情報記録媒体２０のメモリ部２２に格納されているとした場合は、セキュリティモジュール２３は、手順Ｐ４６として、上記メモリ部２２から上記読み出した値Ｅnc（Kst，Kco）をストレージ鍵Ｋstを用いて復号して暗号鍵Ｋcoを得、さらに、この暗号鍵Ｋcoをセッション鍵Ｋseで暗号化した値Ｅnc（Kse，Kco）を、手順Ｐ５７としてメモリ記録再生装置２００に送る。メモリ記録再生装置２００は、当該値Ｅnc（Kse，Kco）をセッション鍵Ｋseを用いて復号することにより暗号鍵Ｋcoを得る。

【０２２７】

その後、セキュリティモジュール２３は、手順Ｐ４８として、暗号化されているコンテンツデータＥnc（Kco，data）をメモリ情報記録媒体２０のメモリ部２２から読み出し、このデータＥnc（Kco，data）をメモリ記録再生装置２００に送信する。メモリ記録再生装置２００では、先に取得した暗号鍵Ｋcoを用いて、上記データＥnc（Kco，data）を復号する。

【０２２８】

なお、上記リボケーションリストの伝送は、上記コンテンツデータの伝送の合間、または終了後に行ってもよい。

【０２２９】

次に、図２１には、第２の実施の形態においてデータの再生を行う場合において、前記第１の実施の形態の図１１の例と同様に、先にリボケーションリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のリボケーションリストを用いて相手方のＩＤが掲載されているか否かを検証するようにしたときの手順を示す。

【０２３０】

なお、図２１の手順Ｐ５１～手順Ｐ５５までは、前述した第１の実施の形態における図１１の手順Ｐ２１～手順Ｒ２５までと略々同じである。

【０２３１】

この図２１において、メモリ記録再生装置２００は、手順Ｐ５１として、乱数

R_Bを再生コマンドと共にセキュリティモジュール２３に送る。上記再生コマンドと乱数R_Bを受け取ったセキュリティモジュール２３は、手順Ｐ５２として、乱数R_AとK_Aを生成し、$V_A=K_A \cdot G$の計算を行い、さらに、前記同様に乱数R_A、乱数R_B、値V_A、バージョンナンバー$RevV_A$からなるビット列にデジタル署名を行ってSig_Aを生成し、それらR_A, R_B, V_A, $RevV_A$, Sig_Aと証明書$Cert_A$をメモリ記録再生装置２００に送る。

【０２３２】

上記セキュリティモジュール２３から$Cert_A$, R_A, R_B, V_A, $RevV_A$, Sig_Aを受け取ると、メモリ記録再生装置２００は、証明書$Cert_A$、デジタル署名Sig_Aの検証を行う。上記証明書$Cert_A$の検証をパスできないときには、メモリ記録再生装置２００は、メモリ情報記録媒体２０を不正な媒体とみなして当該プロトコルを終了し、一方で、当該検証において正当であると判定された場合は上記証明書$Cert_A$からパブリック鍵$PubKey_A$を手に入れる。次に、メモリ記録再生装置２００は、セキュリティモジュール２３から返送されてきた乱数R_Bと先の手順Ｒ５１で生成した乱数R_Bとが等しく、且つデジタル署名Sig_Aが正当であると判定されたときには、次の処理に進み、そうでない場合にはセキュリティモジュール２３を備えたメモリ情報記録媒体２０が不正な媒体であると判断して当該プロトコルを終了する。

【０２３３】

上記セキュリティモジュール２３から返送されてきた乱数R_Bと先に生成したものとが等しく、且つデジタル署名Sig_Aが正当であると判定されたとき、メモリ記録再生装置２００は、手順Ｐ５３として、K_Bを生成し、$V_B=K_B \cdot G$の計算を行い、更に、上記乱数R_B、乱数R_A、値V_B、バージョンナンバー$RevV_B$からなるビット列にデジタル署名を行ってSig_Bを生成し、これらR_B, R_A, V_B, $RevV_B$, Sig_Bと証明書$Cert_B$をセキュリティモジュール２３に送る。

【０２３４】

上記メモリ記録再生装置２００から$Cert_B$, R_B, R_A, V_B, $RevV_B$, Sig_Bを受け取ると、セキュリティモジュール２３は、メモリ記録再生装置２００の証明書$Cert_B$、デジタル署名Sig_Bの検証を行う。上記証明書$Cert_B$の検証をパス

できないとき、セキュリティモジュール２３は、そのメモリ記録再生装置２００を不正な装置とみなして当該プロトコルを終了し、一方で、当該検証で正当であると判定した場合には、上記証明書$Cert_B$からパブリック鍵$PubKey_B$を手に入れる。次に、セキュリティモジュール２３は、メモリ記録再生装置２００から返送されてきた乱数R_Aと先の手順Ｒ５２で生成した乱数R_Aとが等しく、且つデジタル署名Sig_Bが正当であると判定されたときには、次の処理に進み、そうでない場合にはメモリ記録再生装置２００が不正な装置であると判断して当該プロトコルを終了する。

【０２３５】

上述のように、セキュリティモジュール２３とメモリ記録再生装置２００の両者が共に正当であると検証された場合、セキュリティモジュール２３とメモリ記録再生装置２００は、前記セッション鍵Ｋseを生成して共有する。

【０２３６】

また、セキュリティモジュール２３とメモリ記録再生装置２００の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール２１３とメモリ記録再生装置２００は、それぞれ相手方が持っているリボケーションリストのバージョンナンバーのチェックを行う。

【０２３７】

ここで、両者のバージョンナンバーが同じである場合、メモリ記録再生装置２００とセキュリティモジュール２３は、それぞれが保持するリボケーションリストを用いて相手方のＩＤの検証を行い、互いに相手方のＩＤがリボケーションリストに掲載されていないことを検証する。

【０２３８】

一方、セキュリティモジュール２３とメモリ記録再生装置２００においてそれぞれ相手方が持っているリボケーションリストのバージョンナンバーのチェックを行った結果、何れか一方の保持しているバージョンよりも他方のバージョンが新しい場合、手順Ｐ５４又はＰ５５として、上記新しいバージョンのリボケーションリストを相手方に送り、この新しいバージョンのリボケーションリストを受け取った側では当該新しいバージョンのリボケーションリストを用いて相手方の

ＩＤ検証を行うと共に、古いバージョンのリボケーションリストを更新する。

【０２３９】

手順Ｐ５６～Ｐ５９は、図２０の手順Ｐ４６～Ｐ４９と同じであるためその説明は省略する。

【０２４０】

次に、当該第２の実施の形態におけるデータ再生の手順として、図２２に示すように、図１８に示したデータ記録時の手順に準ずる手順を用いることも可能である。なお、図２１の手順Ｐ６１～Ｐ６４については、図１９の手順Ｐ３１～Ｐ３４と同じであるためその説明は省略する。

【０２４１】

この図２２の例において、セキュリティモジュール２３は、手順Ｐ６５として、メモリ部２２から読み取った前記暗号化されているコンテンツデータＥnc（Kco, data）を、暗号鍵Kcoを用いて復号し、その復号後のデータをセッション鍵Kseを用いて暗号化する。セキュリティモジュール２３は、当該セッション鍵Kseを用いて暗号化されたコンテンツデータＥnc（Kse, data）を、手順Ｐ６６として、メモリ記録再生装置２００に送信する。

【０２４２】

メモリ記録再生装置２００は、上記データＥnc（Kse, data）を、自己が保持するセッション鍵Kseにて復号する。これにより、メモリ記録再生装置２００は、復号後のコンテンツデータを得る。

【０２４３】

このようにすることで、セキュリティモジュール２３はデータを暗号化している暗号鍵Ｋｃｏをメモリ記録再生装置２００に教える必要がなくなる（暗号鍵Kcoが外部に出力することがなくなる）。

【０２４４】

以上説明した第１、第２の実施の形態では、秘密鍵が露呈してしまった情報記録媒体或いは記録再生装置のＩＤ（リボークされる機器又は媒体のＩＤ）のリストを用いて、不正に情報が複製等されることを防止した例を挙げたが、本発明では、正当な情報記録媒体或いは記録再生装置を示すレジストレーションリストを

用いることで、上述同様に不正に情報が複製等されることを防止することも可能である。

【０２４５】

すなわち、レジストレーションリストは、登録リスト、正直者リストとも呼ばれ、システム全体若しくはその中の一部であるサブシステムにおいて、正当な情報記録媒体もしくは記録再生装置であるとセンタＴＣが判断したもののＩＤをリストアップし、それにデジタル署名を施したものである。

【０２４６】

当該レジストレーションリストは、図２３に示すように、例えば単調増加する番号であって当該レジストレーションリストのバージョンを示すバージョンナンバーと、正当な情報記録媒体或いは記録再生装置のＩＤ（登録された機器又は媒体のＩＤ）のリストと、センタＴＣによるデジタル署名とからなるものである。このレジストレーションリストの登録は、一例として、あるホームネットワーク内の装置および記録媒体のＩＤを、そのネットワーク内の一つのの装置がリストアップしてセンタＴＣに送信し、センタＴＣがこれらの全ての記録媒体及び装置が正当なものであると判断したとき、このリストに対しデジタル署名を付加して送り返し、これを受け取った装置がホームネットワーク内にこのリストを配布するようなことにより行われる。これにより、そのホームネットワーク内で信頼できる装置及び記録媒体全てのＩＤを各装置と記録媒体は知ることができるようになり、当該レジストレーションリストにリストアップされているＩＤを持つエンティティ（装置や媒体）のみを信用してプロトコルを行うことが可能となる。言い換えれば、秘密鍵が露呈してしまった記録媒体又は装置、及びそれを用いて不正に複製された記録媒体又は不正に製造された装置については、レジストレーションリストに掲載されないことになり、したがってそれら不正な装置や媒体をこのシステムから排除することが可能になる。また、記録再生装置を工場から出荷する際には、最新版のレジストレーションリストを不揮発性メモリに格納して出荷する。

【０２４７】

以下、上記レジストレーションリストを使用した第３の実施の形態について説

明する。

【０２４８】

第３の実施の形態は、前述の第１の実施の形態で説明した光ディスク情報記録媒体１０のセキュリティモジュール１３の不揮発性メモリ３４と、光ディスク記録再生装置１００の不揮発性メモリ１１０に、前記リボケーションリストに代えて上記レジストレーションリストを格納するようにした例である。当該第３の実施の形態における光ディスク情報記録媒体１０、光ディスク記録再生装置１００の構成は、前記図１～図３と同じであるため、それら構成についての説明は省略する。

【０２４９】

図２４から図２６を用いて、第３の実施の形態の光ディスク記録再生装置１００が光ディスク情報記録媒体１０にデータを記録する手順を説明する。なお、図２４～図２６は、前記第１の実施の形態の図６～図８と略々同様な図面であり、各手順についても略々同じであるため、以下の説明では、前記図６～図８とは異なる部分のみ説明する。

【０２５０】

図２４は前記図６と略々同様な手順を表しており、手順Ｒ２として、光ディスク記録再生装置１００とセキュリティモジュール１３との間でレジストレーションリストのバージョンナンバーを交換する。

【０２５１】

また、手順Ｒ３，Ｒ４では、何れかの一方が他方のレジストレーションリストより新しいレジストレーションリストを持っていた場合、当該新しいレジストレーションリストを持っている方は自分のレジストレーションリストを他方に送る。一方、古いレジストレーションリストを持っている方は、新しいレジストレーションリストを持っている方から、当該新しいレジストレーションリストを送ってもらい、その正当性を検証した後、自分が持つレジストレーションリストを、その送られてきた新しいレジストレーションリストに更新する。

【０２５２】

なお、手順Ｒ３，Ｒ４におけるレジストレーションリストの送付は、後の手順

Ｒ５におけるデータの記録と順序が前後してもかまわない。つまり、手順Ｒ５にてデータの記録を行った後に、手順Ｒ３或いはＲ４でのレジストレーションリストの送付を行うようにしてもよい。

【０２５３】

次に、図２５には、上記図２４に示した第３の実施の形態の光ディスク記録再生装置１００が光ディスク情報記録媒体１０にデータを記録するまでの手順の詳細を示しており、前記図７と略々同様な手順となっている。

【０２５４】

この図２５において、手順Ｒ１２の際のセキュリティモジュール１３は、乱数R_A、乱数R_B、値V_A、レジストレーションリストのバージョンナンバー$RegV_A$からなるビット列$R_A||R_B||V_A||RegV_A$にデジタル署名の関数Signを用いたデジタル署名を行い$Sig_A=Sign\ (PriKey_A,\ R_A||R_B||V_A||RegV_A)$を得る。セキュリティモジュール１３は、これら$R_A$，$R_B$，$V_A$，$RegV_A$，$Sig_A$に証明書$Cert_A$を付け、光ディスク記録再生装置１００に送る。なお、セキュリティモジュール１３がレジストレーションリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして０を用いる。

【０２５５】

これら$Cert_A$，R_A，R_B，V_A，$RegV_A$，Sig_Aを受け取った光ディスク記録再生装置１００は、証明書$Cert_A$、デジタル署名Sig_A、ID_Aの検証を行い、その検証をパスし、さらに、セキュリティモジュールから返送されてきた乱数R_Bと先に生成したものとが等しく、且つデジタル署名Sig_Aが正当であると判定されたとき、自己の不揮発性メモリ１１０に格納しているレジストレーションリストを用い、光ディスク情報記録媒体１０のID_Aが当該レジストレーションリストに登録されていることを検証する。この検証の結果、光ディスク情報記録媒体１０のID_Aがレジストレーションリストに登録されていない場合には、当該光ディスク情報記録媒体１０は不正な媒体であると判定し、当該プロトコルを終了する。

【０２５６】

一方、上記ID_Aが当該レジストレーションリストに登録されており、その光

ディスク情報記録媒体１０が正当であると判断した場合、光ディスク記録再生装置１００は、手順Ｒ１３として、K_Bを生成し、$V_B = K_B \cdot G$の計算を行い、更に、上記乱数R_B、乱数R_A、値V_B、当該装置１００が持つレジストレーションリストのバージョンナンバー$RegV_B$からなるビット列$R_B||R_A||V_B||RegV_B$にデジタル署名を行って$Sig_B = Sign(PriKey_B, R_B||R_A||V_B||RegV_B)$を得る。光ディスク記録再生装置１００は、これら$R_B$, R_A, V_B, $RegV_B$, Sig_Bに証明書$Cert_B$を付け、セキュリティモジュール１３に送る。なお、光ディスク記録再生装置１００がレジストレーションリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして０を用いる。

【０２５７】

上記光ディスク記録再生装置１００から$Cert_B$, R_B, R_A, V_B, $RegV_B$, Sig_Bを受け取ると、セキュリティモジュール１３は、証明書$Cert_B$、デジタル署名Sig_B、ID_Bの検証を行い、その検証をパスした時、自己の不揮発性メモリ３４に格納しているレジストレーションリストを用い、光ディスク記録再生装置１００のID_Bが当該レジストレーションリストに登録されていることを検証する。この検証の結果、光ディスク記録再生装置１００のID_Bがレジストレーションリストに登録されていない場合には、当該光ディスク記録再生装置１００は不正な装置であると判定し、当該プロトコルを終了する。

【０２５８】

一方、光ディスク記録再生装置１００のID_Bが当該レジストレーションリストに登録されており、その光ディスク記録再生装置１００が正当であると判断した場合、すなわち、セキュリティモジュール１３と光ディスク記録再生装置１００の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール１３と光ディスク記録再生装置１００はセッション鍵Ksesを生成して共有する。

【０２５９】

次に、セキュリティモジュール１３と光ディスク記録再生装置１００は、それぞれ相手方が持っているレジストレーションリストのバージョンナンバーのチェックを行い、自己の保持しているバージョンよりも新しい場合、手順Ｒ１４又は

Ｒ１５として、その新しいバージョンのレジストレーションリストを相手方に送る。上述のように、相手方から新しいバージョンナンバーのレジストレーションリストが送られてきた方は、当該レジストレーションリスト内に含まれるセンタＴＣの署名ＴＣSigを検証し、その検証をパスしたとき、その新しいレジストレーションリストを用いて自己が保持している古いレジストレーションリストを更新（リストのアップデート）する。

【０２６０】

その後の手順Ｒ１６以降は、前記図７の場合と同様である。

【０２６１】

なお、上記レジストレーションリストの伝送は、コンテンツデータの伝送の合間、または終了後に行ってもよい。

【０２６２】

図２６には、前記第１の実施の形態における図８の手順を、レジストレーションリストにも適用した例を示している。すなわち、図２６は、先にレジストレーションリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のレジストレーションリストを用いて相手方のＩＤを検証するようにした場合の、データ記録時の手順を示している。

【０２６３】

この図２６において、手順Ｒ２２の際のセキュリティモジュール１３は、乱数R_A、乱数R_B、値V_A、レジストレーションリストのバージョンナンバー$RegV_A$からなるビット列$R_A||R_B||V_A||RegV_A$にデジタル署名を行ってSig_Aを得、これらR_A，R_B，V_A，$RegV_A$，Sig_Aに証明書$Cert_A$を付けて光ディスク記録再生装置１００に送る。

【０２６４】

これら$Cert_A$，R_A，R_B，V_A，$RegV_A$，Sig_Aを受け取った光ディスク記録再生装置１００は、証明書$Cert_A$、デジタル署名Sig_Aの検証を行い、その検証をパスし、さらに、セキュリティモジュール１３から返送されてきた乱数R_Bと先に生成したものとが等しく、且つデジタル署名Sig_Aが正当であると判定されたとき、手順Ｒ２３として、K_Bを生成し、$V_B=K_B \cdot G$の計算を行い、更に、

上記乱数R_B、乱数R_A、値V_B、当該装置１００が持つレジストレーションリストのバージョンナンバー$RegV_B$からなるビット列にデジタル署名を行ってSig_Bを得る。光ディスク記録再生装置１００は、これらR_B，R_A，V_B，$RegV_B$，Sig_Bに証明書$Cert_B$を付け、セキュリティモジュール１３に送る。

【０２６５】

上記光ディスク記録再生装置１００から$Cert_B$，R_B，R_A，V_B，$RegV_B$，Sig_Bを受け取ると、セキュリティモジュール１３は、証明書$Cert_B$、デジタル署名Sig_Bの検証を行い、その検証をパスした時、次の処理に進む。

【０２６６】

上述のように、セキュリティモジュール１３と光ディスク記録再生装置１００の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール１３と光ディスク記録再生装置１００は、セッション鍵Ｋseを生成して共有する。

【０２６７】

また、セキュリティモジュール１３と光ディスク記録再生装置１００の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール１３と光ディスク記録再生装置１００は、それぞれ相手方が持っているレジストレーションリストのバージョンナンバーのチェックを行う。

【０２６８】

ここで、両者のバージョンナンバーが同じである場合、光ディスク記録再生装置１００とセキュリティモジュール１３は、それぞれが保持するレジストレーションリストを用いて相手方のＩＤの検証を行い、互いに相手方のＩＤがレジストレーションリストに登録されていることを検証する。このレジストレーションリストの相互検証の結果、両者において共にレジストレーションリストに登録されていると判定された場合には、後段の手順Ｒ２６の処理に進む。また、セキュリティモジュール１３において、光ディスク記録再生装置１００のID_Bが自己のレジストレーションリストに登録されていない場合には、当該光ディスク記録再生装置１００は不正な装置であると判定し、当該プロトコルを終了する。同じく、光ディスク記録再生装置１００において、セキュリティモジュール１３のＩＤ

$_{A}$が自己のレジストレーションリストに登録されていない場合には、当該セキュリティモジュール１３は不正な媒体のものであると判定し、当該プロトコルを終了する。

【０２６９】

一方、セキュリティモジュール１３と光ディスク記録再生装置１００においてそれぞれ相手方が持っているレジストレーションリストのバージョンナンバーのチェックを行った結果、何れか一方の保持しているバージョンよりも他方のバージョンが新しい場合、手順Ｒ２４又はＲ２５として、上記新しいバージョンのレジストレーションリストを相手方に送り、この新しいバージョンのレジストレーションリストを受け取った側では当該新しいバージョンのレジストレーションリストを用いて相手方のＩＤ検証を行うと共に、古いバージョンのレジストレーションリストを更新する。

【０２７０】

その後の手順Ｒ２６以降は、前記図８の場合と同様である。

【０２７１】

次に、図２７～図２９を用いて、上記第３の実施の形態の光ディスク記録再生装置１００が光ディスク１２からデータを再生する手順を説明する。なお、図２７～図２６は、前記第１の実施の形態の図９～図１１と略々同様な図面であり、各手順についても略々同じであるため、以下の説明では、前記図９～図１１とは異なる部分のみ説明する。

【０２７２】

図２７において、光ディスク記録再生装置１００とセキュリティモジュール１３は、手順Ｐ２にて、レジストレーションリストに相手方のＩＤが載せられていないことの確認を互いに行い、自分が持つレジストレーションリストのバージョンナンバーを送り合う。

【０２７３】

また、手順Ｐ３，Ｐ４として、光ディスク記録再生装置１００とセキュリティモジュール１３は、どちらかが相対的に新しいレジストレーションリストを持っていた場合には、それを他方に送り、送られた方はそれを用いて自分のレジスト

レーションリストを更新することも同様である。

【０２７４】

その後の手順Ｐ５以降は、前記図９の場合と同様である。

【０２７５】

次に、図２８には、上記図２７に示した第３の実施の形態の光ディスク記録再生装置１００が光ディスク情報記録媒体１０からデータを再生するまでの手順の詳細を示している。なお、当該図２８の手順は、前記図１０と略々同様な手順となっている。

【０２７６】

この図２８において、手順Ｐ１２の際のセキュリティモジュール１３は、乱数R_A、乱数R_B、値V_A、レジストレーションリストのバージョンナンバー$RegV_A$からなるビット列にデジタル署名を行いSig_Aを得る。セキュリティモジュール１３は、これらに証明書$Cert_A$を付け、光ディスク記録再生装置１００に送る。なお、セキュリティモジュール１３がレジストレーションリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして０を用いる。

【０２７７】

これら$Cert_A$，R_A，R_B，V_A，$RegV_A$，Sig_Aを受け取った光ディスク記録再生装置１００は、証明書$Cert_A$、デジタル署名Sig_A、ID_Aの検証を行い、その検証をパスし、さらに、セキュリティモジュール１３から返送されてきた乱数R_Bと先に生成したものとが等しく、且つデジタル署名Sig_Aが正当であると判定されたとき、自己の不揮発性メモリ１１０に格納しているレジストレーションリストを用い、光ディスク情報記録媒体１０のID_Aが当該レジストレーションリストに登録されていることを検証する。この検証の結果、光ディスク情報記録媒体１０のID_Aがレジストレーションリストに登録されていない場合には、当該光ディスク情報記録媒体１０は不正な媒体であると判定し、当該プロトコルを終了する。

【０２７８】

一方、上記ID_Aが当該レジストレーションリストに登録されており、その光ディスク情報記録媒体１０が正当であると判断した場合、光ディスク記録再生装

置１００は、手順Ｐ１３として、K_Bを生成し、$V_B=K_B \cdot G$の計算を行い、更に、上記乱数R_B、乱数R_A、値V_B、当該装置１００のレジストレーションリストのバージョンナンバー$RegV_B$からなるビット列にデジタル署名を行ってSig_Bを得る。光ディスク記録再生装置１００は、これらR_B，R_A，V_B，$RegV_B$，Sig_Bに証明書$Cert_B$を付け、セキュリティモジュール１３に送る。なお、光ディスク記録再生装置１００がレジストレーションリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして０を用いる。

【０２７９】

上記光ディスク記録再生装置１００から$Cert_B$，R_B，R_A，V_B，$RegV_B$，Sig_Bを受け取ると、セキュリティモジュール１３は、証明書$Cert_B$、デジタル署名Sig_B、ID_Bの検証を行い、その検証をパスした時、自己の不揮発性メモリ３４に格納しているレジストレーションリストを用い、光ディスク記録再生装置１００のID_Bが当該レジストレーションリストに登録されていることを検証する。この検証の結果、光ディスク記録再生装置１００のID_Bがレジストレーションリストに登録されていない場合には、当該光ディスク記録再生装置１００は不正な装置であると判定し、当該プロトコルを終了する。

【０２８０】

一方、光ディスク記録再生装置１００のID_Bが当該レジストレーションリストに登録されており、その光ディスク記録再生装置１００が正当であると判断した場合、すなわち、セキュリティモジュール１３と光ディスク記録再生装置１００の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール１３と光ディスク記録再生装置１００はセッション鍵Kseを生成して共有する。

【０２８１】

次に、セキュリティモジュール１３と光ディスク記録再生装置１００は、それぞれ相手方が持っているレジストレーションリストのバージョンナンバーのチェックを行い、自己の保持しているバージョンよりも新しい場合、手順Ｐ１４又はＰ１５として、その新しいバージョンのレジストレーションリストを相手方に送る。上述のように、相手方から新しいバージョンナンバーのレジストレーション

リストが送られてきた方は、当該レジストレーションリスト内に含まれるセンタＴＣの署名ＴＣSigを検証し、その検証をパスしたとき、その新しいレジストレーションリストを用いて自己が保持している古いレジストレーションリストを更新（リストのアップデート）する。

【０２８２】

その後の手順Ｐ１６以降は、前記図１０の場合と同様である。

【０２８３】

なお、上記レジストレーションリストの伝送は、コンテンツデータの伝送の合間、または終了後に行ってもよい。

【０２８４】

~~図２９には、前記第１の実施の形態における図１１の手順を、レジストレーション~~リストにも適用した例を示している。すなわち、図２９は、先にレジストレーションリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のレジストレーションリストを用いて相手方のＩＤを検証するようにした場合の、データ再生時の手順を示している。

【０２８５】

この図２９において、手順Ｐ２２の際のセキュリティモジュール１３は、乱数R_A、乱数R_B、値V_A、レジストレーションリストのバージョンナンバー$RegV_A$からなるビット列にデジタル署名を行ってSig_Aを得、これらに証明書$Cert_A$を付けて光ディスク記録再生装置１００に送る。

【０２８６】

それらを受け取った光ディスク記録再生装置１００は、証明書$Cert_A$、デジタル署名Sig_Aの検証を行い、その検証をパスし、さらに、セキュリティモジュール１３から返送されてきた乱数R_Bと先に生成したものとが等しく、且つデジタル署名Sig_Aが正当であると判定されたとき、手順Ｐ２３として、K_Bを生成し、$V_B=K_B \cdot G$の計算を行い、更に、上記乱数R_B、乱数R_A、値V_B、当該装置１００が持つレジストレーションリストのバージョンナンバー$RegV_B$からなるビット列にデジタル署名を行ってSig_Bを得る。光ディスク記録再生装置１００は、これらR_B，R_A，V_B，$RegV_B$，Sig_Bに証明書$Cert_B$を付け、セキュリティ

モジュール１３に送る。上記光ディスク記録再生装置１００から$Cert_B$, R_B, R_A, V_B, $RegV_B$, Sig_Bを受け取ると、セキュリティモジュール１３は、証明書$Cert_B$、デジタル署名Sig_Bの検証を行い、その検証をパスした時、次の処理に進む。

【０２８７】

セキュリティモジュール１３と光ディスク記録再生装置１００の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール１３と光ディスク記録再生装置１００は、セッション鍵Ksesを生成して共有する。また、セキュリティモジュール１３と光ディスク記録再生装置１００の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール１３と光ディスク記録再生装置１００は、それぞれ相手方が持っているレジストレーションリストのバージョンナンバーのチェックを行う。

【０２８８】

両者のバージョンナンバーが同じである場合、光ディスク記録再生装置１００とセキュリティモジュール１３は、それぞれが保持するレジストレーションリストを用いて相手方のＩＤの検証を行い、互いに相手方のＩＤがレジストレーションリストに登録されていることを検証する。このレジストレーションリストの相互検証の結果、両者において共にレジストレーションリストに登録されていると判定された場合には、後段の手順Ｐ２６の処理に進む。また、セキュリティモジュール１３において、光ディスク記録再生装置１００のID_Bが自己のレジストレーションリストに登録されていない場合には、当該光ディスク記録再生装置１００は不正な装置であると判定し、当該プロトコルを終了する。同じく、光ディスク記録再生装置１００において、セキュリティモジュール１３のID_Aが自己のレジストレーションリストに登録されていない場合には、当該セキュリティモジュール１３は不正な媒体のものであると判定し、当該プロトコルを終了する。

【０２８９】

一方、セキュリティモジュール１３と光ディスク記録再生装置１００においてそれぞれ相手方が持っているレジストレーションリストのバージョンナンバーのチェックを行った結果、何れか一方の保持しているバージョンよりも他方のバー

ジョンが新しい場合、手順Ｐ２４又はＰ２５として、上記新しいバージョンのレジストレーションリストを相手方に送り、この新しいバージョンのレジストレーションリストを受け取った側では当該新しいバージョンのレジストレーションリストを用いて相手方のＩＤ検証を行うと共に、古いバージョンのレジストレーションリストを更新する。

【０２９０】

その後の手順Ｐ２６以降は、前記図１１の場合と同様である。

【０２９１】

次に、本発明の第４の実施の形態について説明する。

【０２９２】

第４の実施の形態は、前述の第２の実施の形態で説明したメモリ情報記録媒体２０のセキュリティモジュール２３の不揮発性メモリ４４と、メモリ記録再生装置２００の不揮発性メモリ２１０に、前記リボケーションリストに代えて上記レジストレーションリストを格納するようにした例である。当該第４の実施の形態におけるメモリ情報記録媒体２０、メモリ記録再生装置２００の構成は、前記図１２～図１４と同じであるため、それら構成についての説明は省略する。

【０２９３】

図３０～図３４を用いて、第４の実施の形態のメモリ記録再生装置２００がメモリ情報記録媒体２０にデータを記録する手順を説明する。なお、図３０～図３４は、前記第２の実施の形態の図１５～図１８と略々同様な図面であり、各手順についても略々同じであるため、以下の説明では、前記図１５～図１８とは異なる部分のみ説明する。

【０２９４】

図３０は前記図１５と略々同様な手順を表しており、手順Ｒ３２として、メモリ記録再生装置２００とセキュリティモジュール２３との間でレジストレーションリストのバージョンナンバーを交換する。

【０２９５】

また、手順Ｒ３３，Ｒ３４では、何れかの一方が他方のレジストレーションリストより新しいレジストレーションリストを持っていた場合、当該新しいレジス

トレーションリストを持っている方は自分のレジストレーションリストを他方に送る。一方、古いレジストレーションリストを持っている方は、新しいレジストレーションリストを持っている方から、当該新しいレジストレーションリストを送ってもらい、その正当性を検証した後、自分が持つレジストレーションリストを、その送られてきた新しいレジストレーションリストに更新する。

【０２９６】

なお、手順Ｒ３３，Ｒ３４におけるレジストレーションリストの送付は、後の手順Ｒ５におけるデータの記録と順序が前後してもかまわない。つまり、手順Ｒ３５にてデータの記録を行った後に、手順Ｒ３３或いはＲ３４でのレジストレーションリストの送付を行うようにしてもよい。

【０２９７】

次に、図３１には、上記図３０に示した第４の実施の形態のメモリ記録再生装置２００がメモリ情報記録媒体２０にデータを記録するまでの手順の詳細を示しており、前記図１６と略々同様な手順となっている。

【０２９８】

この図３１において、手順Ｒ４２の際のセキュリティモジュール２３は、乱数R_A、乱数R_B、値V_A、レジストレーションリストのバージョンナンバー$RegV_A$からなるビット列にデジタル署名を行いSig_Aを得る。セキュリティモジュール２３は、これらに証明書$Cert_A$を付け、メモリ記録再生装置２００に送る。なお、セキュリティモジュール２３がレジストレーションリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして０を用いる。

【０２９９】

それら$Cert_A$，R_A，R_B，V_A，$RegV_A$，Sig_Aを受け取ったメモリ記録再生装置２００は、証明書$Cert_A$、デジタル署名Sig_A、ID_Aの検証を行い、その検証をパスし、さらに、セキュリティモジュール２３から返送されてきた乱数R_Bと先に生成したものとが等しく、且つデジタル署名Sig_Aが正当であると判定されたとき、自己の不揮発性メモリ２１０に格納しているレジストレーションリストを用い、メモリ情報記録媒体２０のID_Aが当該レジストレーションリストに登録されていることを検証する。この検証の結果、メモリ情報記録媒体２０のＩ

D_Aがレジストレーションリストに登録されていない場合には、当該メモリ情報記録媒体２０は不正な媒体であると判定し、当該プロトコルを終了する。

【０３００】

一方、上記ID_Aが当該レジストレーションリストに登録されており、そのメモリ情報記録媒体２０が正当であると判断した場合、メモリ記録再生装置２００は、手順Ｒ４３として、K_Bを生成し、$V_B=K_B \cdot G$の計算を行い、更に、上記乱数R_B、乱数R_A、値V_B、当該装置２００が持つレジストレーションリストのバージョンナンバー$RegV_B$からなるビット列にデジタル署名を行ってSig_Bを得る。メモリ記録再生装置２００は、これらに証明書$Cert_B$を付け、セキュリティモジュール２３に送る。なお、メモリ記録再生装置２００がレジストレーションリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして０を用いる。

【０３０１】

上記メモリ記録再生装置２００から$Cert_B$, R_B, R_A, V_B, $RegV_B$, Sig_Bを受け取ると、セキュリティモジュール２３は、証明書$Cert_B$、デジタル署名Sig_B、ID_Bの検証を行い、その検証をパスした時、自己の不揮発性メモリ４４に格納しているレジストレーションリストを用い、メモリ記録再生装置２００のID_Bが当該レジストレーションリストに登録されていることを検証する。この検証の結果、メモリ記録再生装置２００のID_Bがレジストレーションリストに登録されていない場合には、当該メモリ記録再生装置２００は不正な装置であると判定し、当該プロトコルを終了する。

【０３０２】

一方、メモリ記録再生装置２００のID_Bが当該レジストレーションリストに登録されており、そのメモリ記録再生装置２００が正当であると判断した場合、すなわち、セキュリティモジュール２３とメモリ記録再生装置２００の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール２３とメモリ記録再生装置２００はセッション鍵Ｋseを生成して共有する。

【０３０３】

次に、セキュリティモジュール２３とメモリ記録再生装置２００は、それぞれ

相手方が持っているレジストレーションリストのバージョンナンバーのチェックを行い、自己の保持しているバージョンよりも新しい場合、手順Ｒ４４又はＲ４５として、その新しいバージョンのレジストレーションリストを相手方に送る。上述のように、相手方から新しいバージョンナンバーのレジストレーションリストが送られてきた方は、当該レジストレーションリスト内に含まれるセンタＴＣの署名ＴＣSigを検証し、その検証をパスしたとき、その新しいレジストレーションリストを用いて自己が保持している古いレジストレーションリストを更新（リストのアップデート）する。

【０３０４】

その後の手順Ｒ４６以降は、前記図１６の場合と同様である。

【０３０５】

なお、上記レジストレーションリストの伝送は、コンテンツデータの伝送の合間、または終了後に行ってもよい。

【０３０６】

図３２には、前記第２の実施の形態における図１７の手順を、レジストレーションリストにも適用した例を示している。すなわち、図３２は、先にレジストレーションリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のレジストレーションリストを用いて相手方のＩＤを検証するようにした場合の、データ記録時の手順を示している。

【０３０７】

この図３２において、手順Ｒ５２の際のセキュリティモジュール２３は、乱数R_A、乱数R_B、値V_A、レジストレーションリストのバージョンナンバー$RegV_A$からなるビット列にデジタル署名を行ってSig_Aを得、これらに証明書$Cert_A$を付けてメモリ記録再生装置２００に送る。

【０３０８】

これら$Cert_A$，R_A，R_B，V_A，$RegV_A$，Sig_Aを受け取ったメモリ記録再生装置２００は、証明書$Cert_A$、デジタル署名Sig_Aの検証を行い、その検証をパスし、さらに、セキュリティモジュール２３から返送されてきた乱数R_Bと先に生成したものとが等しく、且つデジタル署名Sig_Aが正当であると判定されたと

き、手順Ｒ５３として、K_Bを生成し、$V_B=K_B \cdot G$の計算を行い、更に、上記乱数R_B、乱数R_A、値V_B、当該装置２００が持つレジストレーションリストのバージョンナンバー$RegV_B$からなるビット列にデジタル署名を行ってSig_Bを得る。メモリ記録再生装置２００は、これらR_B, R_A, V_B, $RegV_B$, Sig_Bに証明書$Cert_B$を付け、セキュリティモジュール２３に送る。

【０３０９】

上記メモリ記録再生装置２００から$Cert_B$, R_B, R_A, V_B, $RegV_B$, Sig_Bを受け取ると、セキュリティモジュール２３は、証明書$Cert_B$、デジタル署名Sig_Bの検証を行い、その検証をパスした時、次の処理に進む。

【０３１０】

上述のように、セキュリティモジュール２３とメモリ記録再生装置２００の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール２３とメモリ記録再生装置２００は、セッション鍵Ｋseを生成して共有する。

【０３１１】

また、セキュリティモジュール２３とメモリ記録再生装置２００の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール２３とメモリ記録再生装置２００は、それぞれ相手方が持っているレジストレーションリストのバージョンナンバーのチェックを行う。

【０３１２】

ここで、両者のバージョンナンバーが同じである場合、メモリ記録再生装置２００とセキュリティモジュール２３は、それぞれが保持するレジストレーションリストを用いて相手方のＩＤの検証を行い、互いに相手方のＩＤがレジストレーションリストに登録されていることを検証する。このレジストレーションリストの相互検証の結果、両者において共にレジストレーションリストに登録されていると判定された場合には、後段の手順Ｒ５６の処理に進む。また、セキュリティモジュール２３において、メモリ記録再生装置２００のID_Bが自己のレジストレーションリストに登録されていない場合には、当該メモリ記録再生装置２００は不正な装置であると判定し、当該プロトコルを終了する。同じく、メモリ記録再生装置２００において、セキュリティモジュール２３のID_Aが自己のレジス

トレーションリストに登録されていない場合には、当該セキュリティモジュール２３は不正な媒体のものであると判定し、当該プロトコルを終了する。

【０３１３】

一方、セキュリティモジュール２３とメモリ記録再生装置２００においてそれぞれ相手方が持っているレジストレーションリストのバージョンナンバーのチェックを行った結果、何れか一方の保持しているバージョンよりも他方のバージョンが新しい場合、手順Ｒ５４又はＲ５５として、上記新しいバージョンのレジストレーションリストを相手方に送り、この新しいバージョンのレジストレーションリストを受け取った側では当該新しいバージョンのレジストレーションリストを用いて相手方のＩＤ検証を行うと共に、古いバージョンのレジストレーションリストを更新する。

【０３１４】

その後の手順Ｒ５６以降は、前記図１７の場合と同様である。

【０３１５】

次に、この第４の実施の形態において、メモリ情報記録媒体２０のメモリ部２２へのデータの記録処理については、前述の図１８と同様の図３３に示すような手順とすることも可能である。

【０３１６】

この図３３において、メモリ記録再生装置２００とセキュリティモジュール２３は、手順Ｒ６２にて相互にレジストレーションリストのバージョンナンバーを交換する。

【０３１７】

また、手順Ｒ６３、Ｒ６４では、レジストレーションリストのバージョンナンバーが古い方を、新しいバージョンナンバーのレジストレーションリストにて更新する。

【０３１８】

手順Ｒ６５以降の処理は、前記図１８と同様である。

【０３１９】

次に、図３４～図３７を用いて、上記第４の実施の形態のメモリ記録再生装置

２００がメモリ情報記録媒体２０のメモリ部２２からデータを再生する手順を説明する。なお、図３４～図３７は、前記第２の実施の形態の図１９～図２２と略々同様な図面であり、各手順についても略々同じであるため、以下の説明では、前記図１９～図２２とは異なる部分のみ説明する。

【０３２０】

図３４において、メモリ記録再生装置２００とセキュリティモジュール２３は、手順Ｐ３２にて、レジストレーションリストに相手方のＩＤが載せられていないことの確認を互いに行い、自分が持つレジストレーションリストのバージョンナンバーを送り合う。

【０３２１】

また、手順Ｐ３３，Ｐ３４として、メモリ記録再生装置２００とセキュリティモジュール２３は、どちらかが相対的に新しいレジストレーションリストを持っていた場合には、それを他方に送り、送られた方はそれを用いて自分のレジストレーションリストを更新することも同様である。

【０３２２】

その後の手順Ｐ３５以降は、前記図１９の場合と同様である。

【０３２３】

次に、図３５には、上記図２０に示した第２の実施の形態のメモリ記録再生装置２００がメモリ情報記録媒体２０のメモリ部２２からデータを再生するまでの手順の詳細を示している。なお、当該図３５の手順は、前記図２０と略々同様な手順となっている。

【０３２４】

この図３５において、手順Ｐ４２の際のセキュリティモジュール２３は、乱数R_A、乱数R_B、値V_A、レジストレーションリストのバージョンナンバー$RegV_A$からなるビット列にデジタル署名を行いSig_Aを得る。セキュリティモジュール２３は、これらに証明書$Cert_A$を付け、メモリ記録再生装置２００に送る。なお、セキュリティモジュール２３がレジストレーションリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして０を用いる。

【０３２５】

これら$Cert_A$，R_A，R_B，V_A，$RegV_A$，Sig_Aを受け取ったメモリ記録再生装置２００は、証明書$Cert_A$、デジタル署名Sig_A、ID_Aの検証を行い、その検証をパスし、さらに、セキュリティモジュール２３から返送されてきた乱数R_Bと先に生成したものとが等しく、且つデジタル署名Sig_Aが正当であると判定されたとき、自己が保持するレジストレーションリストを用い、メモリ情報記録媒体２０のID_Aが当該レジストレーションリストに登録されていることを検証する。この検証の結果、メモリ情報記録媒体２０のID_Aがレジストレーションリストに登録されていない場合には、当該メモリ情報記録媒体２０は不正な媒体であると判定し、当該プロトコルを終了する。

【０３２６】

一方、上記ID_Aが当該レジストレーションリストに登録されており、そのメモリ情報記録媒体２０が正当であると判断した場合、メモリ記録再生装置２００は、手順Ｐ４３として、K_Bの生成と$V_B=K_B \cdot G$の計算を行い、更に、上記乱数R_B、乱数R_A、値V_B、当該装置２００のレジストレーションリストのバージョンナンバー$RegV_B$からなるビット列にデジタル署名を行ってSig_Bを得る。メモリ記録再生装置２００は、これらに証明書$Cert_B$を付け、セキュリティモジュール２３に送る。なお、メモリ記録再生装置２００がレジストレーションリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして０を用いる。

【０３２７】

上記メモリ記録再生装置２００から$Cert_B$，R_B，R_A，V_B，$RegV_B$，Sig_Bを受け取ると、セキュリティモジュール２３は、証明書$Cert_B$、デジタル署名Sig_B、ID_Bの検証を行い、その検証をパスした時、自己が保持するレジストレーションリストを用い、メモリ記録再生装置２００のID_Bが当該レジストレーションリストに登録されていることを検証する。この検証の結果、メモリ記録再生装置２００のID_Bがレジストレーションリストに登録されていない場合には、当該メモリ記録再生装置２００は不正な装置であると判定し、当該プロトコルを終了する。

【０３２８】

一方、メモリ記録再生装置２００のＩＤ$_B$が当該レジストレーションリストに登録されており、そのメモリ記録再生装置２００が正当であると判断した場合、すなわち、セキュリティモジュール２３とメモリ記録再生装置２００の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール２３とメモリ記録再生装置２００はセッション鍵Ｋseを生成して共有する。

【０３２９】

次に、セキュリティモジュール２３とメモリ記録再生装置２００は、それぞれ相手方が持っているレジストレーションリストのバージョンナンバーのチェックを行い、自己の保持しているバージョンよりも新しい場合、手順Ｐ４４又はＰ４５として、その新しいバージョンのレジストレーションリストを相手方に送る。上述のように、相手方から新しいバージョンナンバーのレジストレーションリストが送られてきた方は、当該レジストレーションリスト内に含まれるセンタＴＣの署名ＴＣSigを検証し、その検証をパスしたとき、その新しいレジストレーションリストを用いて自己が保持している古いレジストレーションリストを更新（リストのアップデート）する。

【０３３０】

その後の手順Ｐ４６以降は、前記図２０の場合と同様である。

【０３３１】

なお、上記レジストレーションリストの伝送は、コンテンツデータの伝送の合間、または終了後に行ってもよい。

【０３３２】

図３６には、前記第２の実施の形態における図２１の手順を、レジストレーションリストにも適用した例を示している。すなわち、図３６は、先にレジストレーションリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のレジストレーションリストを用いて相手方のＩＤを検証するようにした場合の、データ再生時の手順を示している。

【０３３３】

この図３６において、手順Ｐ５２の際のセキュリティモジュール２３は、乱数

R_A、乱数R_B、値V_A、バージョンナンバー$RegV_A$からなるビット列にデジタル署名を行ってSig_Aを得、これらに証明書$Cert_A$を付けてメモリ記録再生装置２００に送る。

【０３３４】

それらを受け取ったメモリ記録再生装置２００は、証明書$Cert_A$、デジタル署名Sig_Aの検証を行い、その検証をパスし、さらに、セキュリティモジュール２３から返送されてきた乱数R_Bと先に生成したものとが等しく、且つデジタル署名Sig_Aが正当であると判定されたとき、手順Ｐ５３として、K_Bを生成し、$V_B = K_B \cdot G$の計算を行い、更に、上記乱数R_B、乱数R_A、値V_B、当該装置２００が持つレジストレーションリストのバージョンナンバー$RegV_B$からなるビット列にデジタル署名を行ってSig_Bを得る。メモリ記録再生装置２００は、これらに証明書$Cert_B$を付け、セキュリティモジュール２３に送る。

【０３３５】

上記メモリ記録再生装置２００から$Cert_B$, R_B, R_A, V_B, $RegV_B$, Sig_Bを受け取ると、セキュリティモジュール２３は、証明書$Cert_B$、デジタル署名Sig_Bの検証を行い、その検証をパスした時、次の処理に進む。

【０３３６】

セキュリティモジュール２３とメモリ記録再生装置２００の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール２３とメモリ記録再生装置２００は、セッション鍵Ｋseを生成して共有する。また、セキュリティモジュール２３とメモリ記録再生装置２００の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール２３とメモリ記録再生装置２００は、それぞれ相手方が持っているレジストレーションリストのバージョンナンバーのチェックを行う。

【０３３７】

両者のバージョンナンバーが同じである場合、メモリ記録再生装置２００とセキュリティモジュール２３は、それぞれが保持するレジストレーションリストを用いて相手方のＩＤの検証を行い、互いに相手方のＩＤがレジストレーションリストに登録されていることを検証する。このレジストレーションリストの相互検

証の結果、両者において共にレジストレーションリストに登録されていると判定された場合には、後段の手順Ｐ５６の処理に進む。また、セキュリティモジュール２３において、メモリ記録再生装置２００のＩＤ$_B$が自己のレジストレーションリストに登録されていない場合には、当該メモリ記録再生装置２００は不正な装置であると判定し、当該プロトコルを終了する。同じく、メモリ記録再生装置２００において、セキュリティモジュール２３のＩＤ$_A$が自己のレジストレーションリストに登録されていない場合には、当該セキュリティモジュール２３は不正な媒体のものであると判定し、当該プロトコルを終了する。

【０３３８】

一方、セキュリティモジュール２３とメモリ記録再生装置２００においてそれぞれ相手方が持っているレジストレーションリストのバージョンナンバーのチェックを行った結果、何れか一方の保持しているバージョンよりも他方のバージョンが新しい場合、手順Ｐ５４又はＰ５５として、上記新しいバージョンのレジストレーションリストを相手方に送り、この新しいバージョンのレジストレーションリストを受け取った側では当該新しいバージョンのレジストレーションリストを用いて相手方のＩＤ検証を行うと共に、古いバージョンのレジストレーションリストを更新する。

【０３３９】

その後の手順Ｐ５６以降は、前記図２１の場合と同様である。

【０３４０】

次に、この第４の実施の形態において、メモリ情報記録媒体２０のメモリ部２２からのデータの再生処理については、前述の図２２と同様の図３７に示すような手順とすることも可能である。

【０３４１】

この図３７において、メモリ記録再生装置２００とセキュリティモジュール２３は、手順Ｐ６２にて相互にレジストレーションリストのバージョンナンバーを交換する。

【０３４２】

また、手順Ｐ６３、Ｐ６４では、レジストレーションリストのバージョンナン

バーが古い方を、新しいバージョンナンバーのレジストレーションリストにて更新する。

【０３４３】

手順Ｐ６５以降の処理は、前記図２２と同様である。

【０３４４】

上述した第１及び第２の実施の形態ではリボケーションリストを、第３及び第４の実施の形態ではレジストレーションリストを用いて、不正に情報が複製等されることを防止した例を挙げたが、本発明では、これらリボケーションリストとレジストレーションリストを用いることで、さらに確実に不正な情報複製等を防止することも可能である。

【０３４５】

ここで、リボケーションリストとレジストレーションリストを用いる場合、それら両者を同時に用いることも可能であり、或いは、それらのうち何れか一方を優先的に使用し、他方を使用しないようにすることも可能である。特に、上記何れか一方を優先的に使用する場合は、不正者リストであるリボケーションリストを優先することが望ましい。

【０３４６】

また、両者を同時に用いる場合、それらリストを区別するために、例えば図３８に示すようなリストフォーマットを用いることが可能である。すなわち、この図３８のリストフォーマットは、リボケーションリストとレジストレーションリストの区別と、それらのバージョンナンバーと、秘密鍵が露呈してしまった情報記録媒体或いは記録再生装置のＩＤ（リボークされる機器又は媒体のＩＤ）のリスト、正当な情報記録媒体或いは記録再生装置のＩＤ（登録された機器又は媒体のＩＤ）のリストと、センタＴＣによるデジタル署名とからなるものである。

【０３４７】

以下、上記リボケーションリストとレジストレーションリストを使用した第５の実施の形態について説明する。

【０３４８】

第５の実施の形態は、前述の第１，第３の実施の形態で説明した光ディスク情

報記録媒体１０のセキュリティモジュール１３の不揮発性メモリ３４と、光ディスク記録再生装置１００の不揮発性メモリ１１０に、前記リボケーションリストとレジストレーションリストを格納するようにした例である。当該第５の実施の形態における光ディスク情報記録媒体１０、光ディスク記録再生装置１００の構成は、前記図１～図３と同じであるため、それら構成についての説明は省略する。

【０３４９】

図３９から図４１を用いて、第５の実施の形態の光ディスク記録再生装置１００が光ディスク情報記録媒体１０にデータを記録する手順を説明する。なお、図３９～図４１は、前記第１の実施の形態の図６～図８、第３の実施の形態の図２４～図２６と略々同様な図面であり、各手順についても略々同じであるため、以下の説明では、それらとは異なる部分のみ説明する。

【０３５０】

図３９は前記図６，図２４と略々同様な手順を表しており、手順Ｒ２として、光ディスク記録再生装置１００とセキュリティモジュール１３との間でリボケーションリスト／レジストレーションリスト（以下、適宜、リストと呼ぶ）のバージョンナンバーを交換する。

【０３５１】

また、手順Ｒ３，Ｒ４では、何れかの一方が他方のリボケーションリスト／レジストレーションリストより新しいリストを持っていた場合、当該新しいリストを持っている方は自分のリストを他方に送る。一方、古いリストを持っている方は、新しいリストを持っている方から、当該新しいリストを送ってもらい、その正当性を検証した後、自分が持つリストを、その送られてきた新しいリストに更新する。

【０３５２】

なお、手順Ｒ３，Ｒ４におけるリストの送付は、後の手順Ｒ５におけるデータの記録と順序が前後してもかまわない。つまり、手順Ｒ５にてデータの記録を行った後に、手順Ｒ３或いはＲ４でのリストの送付を行うようにしてもよい。

【０３５３】

次に、図４０には、上記図３９に示した第５の実施の形態の光ディスク記録再生装置１００が光ディスク情報記録媒体１０にデータを記録するまでの手順の詳細を示しており、前記図７、図２５と略々同様な手順となっている。

【０３５４】

この図４０において、手順Ｒ１２の際のセキュリティモジュール１３は、乱数R_A、乱数R_B、値V_A、リボケーションリストのバージョンナンバー$RevV_A$、レジストレーションリストのバージョンナンバー$RegV_A$からなるビット列$R_A||R_B||V_A||RevV_A||RegV_A$にデジタル署名の関数Signを用いたデジタル署名を行い$Sig_A=Sign\ (PriKey_A,\ R_A||R_B||V_A||RevV_A||RegV_A)$を得る。セキュリティモジュール１３は、これら$R_A$, R_B, V_A, $RevV_A$, $RegV_A$, Sig_Aに証明書$Cert_A$を付け、光ディスク記録再生装置１００に送る。なお、セキュリティモジュール１３がリボケーションリスト／レジストレーションリストを持たない場合或いは使用しない場合は、それぞれバージョンナンバーとして０を用いる。

【０３５５】

これら$Cert_A$, R_A, R_B, V_A, $RevV_A$, $RegV_A$, Sig_Aを受け取った光ディスク記録再生装置１００は、証明書$Cert_A$、デジタル署名Sig_A、ID_Aの検証を行い、その検証をパスし、さらに、セキュリティモジュール１３から返送されてきた乱数R_Bと先に生成したものとが等しく、且つデジタル署名Sig_Aが正当であると判定されたとき、自己の不揮発性メモリ１１０に格納しているリボケーションリスト／レジストレーションリストを用い、光ディスク情報記録媒体１０のID_Aが当該リストに載っているか否かを検証する。このときの検証は、上述したように両者のリストを用いても良いし、また、優先的に一方のリスト（特にリボケーションリスト）を用いても良い。この検証の結果、当該光ディスク情報記録媒体１０が不正な媒体であると判定した場合は、当該プロトコルを終了する。

【０３５６】

一方、上記リストを用いた検証の結果、その光ディスク情報記録媒体１０が正当であると判断した場合、光ディスク記録再生装置１００は、手順Ｒ１３として、K_Bを生成し、$V_B=K_B\cdot G$の計算を行い、更に、上記乱数R_B、乱数R_A、値

V_B、当該装置１００が持つリボケーションリストのバージョンナンバー$RevV_B$、レジストレーションリストのバージョンナンバー$RegV_B$からなるビット列$R_B||R_A||V_B||RevV_B||RegV_B$にデジタル署名を行って$Sig_B=Sign(PriKey_B, R_B||R_A||V_B||RevV_B||RegV_B)$を得る。光ディスク記録再生装置１００は、これら$R_B$, R_A, V_B, $RevV_B$, $RegV_B$, Sig_Bに証明書$Cert_B$を付け、セキュリティモジュール１３に送る。なお、光ディスク記録再生装置１００がリボケーションリスト／レジストレーションリストを持たない場合或いは使用しない場合は、それぞれバージョンナンバーとして０を用いる。

【０３５７】

上記光ディスク記録再生装置１００から$Cert_B$, R_B, R_A, V_B, $RevV_B$, $RegV_B$, Sig_Bを受け取ると、セキュリティモジュール１３は、証明書$Cert_B$、デジタル署名Sig_B、ID_Bの検証を行い、その検証をパスした時、自己の不揮発性メモリ３４に格納しているリボケーションリスト／レジストレーションリストを用い、光ディスク記録再生装置１００のID_Bが当該リストに載っているか否かを検証する。このときの検証は、上述したように両者のリストを用いても良いし、また、優先的に一方のリスト（特にリボケーションリスト）を用いても良い。この検証の結果、当該光ディスク記録再生装置１００が不正な媒体であると判定した場合は、当該プロトコルを終了する。

【０３５８】

一方、上記検証の結果、その光ディスク記録再生装置１００が正当であると判断した場合、すなわち、セキュリティモジュール１３と光ディスク記録再生装置１００の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール１３と光ディスク記録再生装置１００はセッション鍵Kseを生成して共有する。

【０３５９】

次に、セキュリティモジュール１３と光ディスク記録再生装置１００は、それぞれ相手方が持っているリボケーションリスト／レジストレーションリストのバージョンナンバーのチェックを行い、自己の保持しているバージョンよりも新しい場合、手順Ｒ１４又はＲ１５として、その新しいバージョンのリストを相手方

に送る。上述のように、相手方から新しいバージョンナンバーのリストが送られてきた方は、当該リスト内に含まれるセンタＴＣの署名ＴＣSigを検証し、その検証をパスしたとき、その新しいリストを用いて自己が保持している古いリストを更新（リストのアップデート）する。

【０３６０】

その後の手順Ｒ１６以降は、前記図７，図２５の場合と同様である。

【０３６１】

なお、上記リボケーションリスト／レジストレーションリストの伝送は、コンテンツデータの伝送の合間、または終了後に行ってもよい。

【０３６２】

~~図４１には、前記第１の実施の形態における図８や、第３の実施の形態における図２６の手順を、本実施の形態のリボケーションリスト／レジストレーションリストにも適用した例を示している。すなわち、図４１は、先にリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のリストを用いて相手方のＩＤを検証するようにした場合の、データ記録時の手順を示している。~~

【０３６３】

この図４１において、手順Ｒ２２の際のセキュリティモジュール１３は、乱数R_A、乱数R_B、値V_A、リボケーションリストのバージョンナンバー$RevV_A$、レジストレーションリストのバージョンナンバー$RegV_A$からなるビット列$R_A||R_B||V_A||RevV_A||RegV_A$にデジタル署名を行って$Sig_A$を得、これら$R_A$，$R_B$，$V_A$，$RevV_A$，$RegV_A$，$Sig_A$に証明書$Cert_A$を付けて光ディスク記録再生装置１００に送る。

【０３６４】

これら$Cert_A$，R_A，R_B，V_A，$RevV_A$，$RegV_A$，Sig_Aを受け取った光ディスク記録再生装置１００は、証明書$Cert_A$、デジタル署名Sig_Aの検証を行い、その検証をパスし、さらに、セキュリティモジュール１３から返送されてきた乱数R_Bと先に生成したものとが等しく、且つデジタル署名Sig_Aが正当であると判定されたとき、手順Ｒ２３として、K_Bを生成し、$V_B=K_B \cdot G$の計算を行い、更に、上記乱数R_B、乱数R_A、値V_B、当該装置１００が持つリボケーションリ

ストのバージョンナンバー$RevV_B$、レジストレーションリストのバージョンナンバー$RegV_B$からなるビット列にデジタル署名を行ってSig_Bを得る。光ディスク記録再生装置１００は、これらR_B，R_A，V_B，$RevV_B$，$RegV_B$，Sig_Bに証明書$Cert_B$を付け、セキュリティモジュール１３に送る。

【０３６５】

上記光ディスク記録再生装置１００から$Cert_B$，R_B，R_A，V_B，$RevV_B$，$RegV_B$，Sig_Bを受け取ると、セキュリティモジュール１３は、証明書$Cert_B$、デジタル署名Sig_Bの検証を行い、その検証をパスした時、次の処理に進む。

【０３６６】

上述のように、セキュリティモジュール１３と光ディスク記録再生装置１００の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール１３と光ディスク記録再生装置１００は、セッション鍵Ｋseを生成して共有する。

【０３６７】

また、セキュリティモジュール１３と光ディスク記録再生装置１００の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール１３と光ディスク記録再生装置１００は、それぞれ相手方が持っているリストのバージョンナンバーのチェックを行う。

【０３６８】

ここで、両者のバージョンナンバーが同じである場合、光ディスク記録再生装置１００とセキュリティモジュール１３は、それぞれが保持するリストを用いて相手方のＩＤの検証を行い、互いに相手方が正当であるか否か検証する。このときの検証は、上述したように両者のリストを用いても良いし、また、優先的に一方のリスト（特にリボケーションリスト）を用いても良い。この検証の結果、両者が共に正当であると判定された場合には、後段の手順Ｒ２６の処理に進む。また、セキュリティモジュール１３において、光ディスク記録再生装置１００が不正な装置であると判定した場合は、当該プロトコルを終了する。同じく、光ディスク記録再生装置１００において、セキュリティモジュール１３が不正な媒体のものであると判定した場合は、当該プロトコルを終了する。

【０３６９】

一方、セキュリティモジュール１３と光ディスク記録再生装置１００においてそれぞれ相手方が持っているリストのバージョンナンバーのチェックを行った結果、何れか一方の保持しているバージョンよりも他方のバージョンが新しい場合、手順Ｒ２４又はＲ２５として、上記新しいバージョンのリストを相手方に送り、この新しいバージョンのリストを受け取った側では当該新しいバージョンのリストを用いて相手方のＩＤ検証を行うと共に、古いバージョンのリストを更新する。

【０３７０】

その後の手順Ｒ２６以降は、前記図８、図２６の場合と同様である。

【０３７１】

次に、図４２～図４４を用いて、上記第５の実施の形態の光ディスク記録再生装置１００が光ディスク１２からデータを再生する手順を説明する。なお、図４２～図４４は、前記第１の実施の形態の図９～図１１、第３の実施の形態の図２７～図２９と略々同様な図面であり、各手順についても略々同じであるため、以下の説明では、前記図９～図１１、図２７～図２９とは異なる部分のみ説明する。

【０３７２】

図４２において、光ディスク記録再生装置１００とセキュリティモジュール１３は、手順Ｐ２にて、リボケーションリスト／レジストレーションリストを用い、互いに相手方が正当なものであることの確認を行い、自分が持つリストのバージョンナンバーを送り合う。

【０３７３】

また、手順Ｐ３，Ｐ４として、光ディスク記録再生装置１００とセキュリティモジュール１３は、どちらかが相対的に新しいリストを持っていた場合には、それを他方に送り、送られた方はそれを用いて自分のリストを更新することも同様である。

【０３７４】

その後の手順Ｐ５以降は、前記図９、図２７の場合と同様である。

【０３７５】

次に、図４３には、上記図４２に示した第５の実施の形態の光ディスク記録再生装置１００が光ディスク情報記録媒体１０からデータを再生するまでの手順の詳細を示している。なお、当該図４３の手順は、前記図１０、図２８と略々同様な手順となっている。

【０３７６】

この図４３において、手順Ｐ１２の際のセキュリティモジュール１３は、乱数R_A、乱数R_B、値V_A、リボケーションリストのバージョンナンバー$RevV_A$、レジストレーションリストのバージョンナンバー$RegV_A$からなるビット列にデジタル署名を行いSig_Aを得る。セキュリティモジュール１３は、これらに証明書$Cert_A$を付け、光ディスク記録再生装置１００に送る。なお、セキュリティモジュール１３がリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして０を用いる。

【０３７７】

これら$Cert_A$，R_A，R_B，V_A，$RevV_A$，$RegV_A$，Sig_Aを受け取った光ディスク記録再生装置１００は、証明書$Cert_A$、デジタル署名Sig_A、ID_Aの検証を行い、その検証をパスし、さらに、セキュリティモジュール１３から返送されてきた乱数R_Bと先に生成したものとが等しく、且つデジタル署名Sig_Aが正当であると判定されたとき、自己の不揮発性メモリ１１０に格納しているリストを用い、光ディスク情報記録媒体１０のID_Aが正当であるか否かを検証する。この検証の結果、光ディスク情報記録媒体１０のID_Aが不正な媒体であると判定された場合は、当該プロトコルを終了する。

【０３７８】

一方、光ディスク情報記録媒体１０が正当であると判断した場合、光ディスク記録再生装置１００は、手順Ｐ１３として、K_Bを生成し、$V_B=K_B \cdot G$の計算を行い、更に、上記乱数R_B、乱数R_A、値V_B、当該装置１００のリボケーションリストのバージョンナンバー$RevV_B$、レジストレーションリストのバージョンナンバー$RegV_B$からなるビット列にデジタル署名を行ってSig_Bを得る。光ディスク記録再生装置１００は、これらR_B，R_A，V_B，$RegV_B$，$RevV_B$，Sig

$_B$に証明書$Cert_B$を付け、セキュリティモジュール１３に送る。なお、光ディスク記録再生装置１００がリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして０を用いる。

【０３７９】

上記光ディスク記録再生装置１００から$Cert_B$, R_B, R_A, V_B, $RevV_B$, $RegV_B$, Sig_Bを受け取ると、セキュリティモジュール１３は、証明書$Cert_B$、デジタル署名Sig_B、ID_Bの検証を行い、その検証をパスした時、自己の不揮発性メモリ３４に格納しているリストを用い、光ディスク記録再生装置１００が正当であるか否か検証する。この検証の結果、光ディスク記録再生装置１００が不正な装置であると判定した場合は、当該プロトコルを終了する。

【０３８０】

一方、光ディスク記録再生装置１００が正当であると判断した場合、すなわち、セキュリティモジュール１３と光ディスク記録再生装置１００の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール１３と光ディスク記録再生装置１００はセッション鍵Ｋseを生成して共有する。

【０３８１】

次に、セキュリティモジュール１３と光ディスク記録再生装置１００は、それぞれ相手方が持っているリストのバージョンナンバーのチェックを行い、自己の保持しているバージョンよりも新しい場合、手順Ｐ１４又はＰ１５として、その新しいバージョンのリストを相手方に送る。上述のように、相手方から新しいバージョンナンバーのリストが送られてきた方は、当該リスト内に含まれるセンタＴＣの署名ＴＣSigを検証し、その検証をパスしたとき、その新しいリストを用いて自己が保持している古いリストを更新（リストのアップデート）する。

【０３８２】

その後の手順Ｐ１６以降は、前記図１０、図２８の場合と同様である。

【０３８３】

なお、上記リストの伝送は、コンテンツデータの伝送の合間、または終了後に行ってもよい。

【０３８４】

図４４には、前記第１の実施の形態における図１１の手順、第３の実施の形態における図２９の手順を、リボケーションリスト／レジストレーションリストにも適用した例を示している。すなわち、図４４は、先にリボケーションリスト／レジストレーションリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のリストを用いて相手方のＩＤを検証するようにした場合の、データ再生時の手順を示している。

【０３８５】

この図４４において、手順Ｐ２２の際のセキュリティモジュール１３は、乱数R_A、乱数R_B、値V_A、リボケーションリストのバージョンナンバー$RevV_A$、レジストレーションリストのバージョンナンバー$RegV_A$からなるビット列にデジタル署名を行ってSig_Aを得、これらに証明書$Cert_A$を付けて光ディスク記録再生装置１００に送る。

【０３８６】

それらを受け取った光ディスク記録再生装置１００は、証明書$Cert_A$、デジタル署名Sig_Aの検証を行い、その検証をパスし、さらに、セキュリティモジュール１３から返送されてきた乱数R_Bと先に生成したものとが等しく、且つデジタル署名Sig_Aが正当であると判定されたとき、手順Ｐ２３として、K_Bを生成し、$V_B=K_B \cdot G$の計算を行い、更に、上記乱数R_B、乱数R_A、値V_B、当該装置１００が持つリボケーションリストンリストのバージョンナンバー$RevV_B$、レジストレーションリストのバージョンナンバー$RegV_B$からなるビット列にデジタル署名を行ってSig_Bを得る。光ディスク記録再生装置１００は、これらR_B，R_A，V_B，$RegV_B$，Sig_Bに証明書$Cert_B$を付け、セキュリ　上記光ディスク記録再生装置１００から$Cert_B$，R_B，R_A，V_B，$RevV_B$，$RegV_B$，Sig_Bを受け取ると、セキュリティモジュール１３は、証明書$Cert_B$、デジタル署名Sig_Bの検証を行い、その検証をパスした時、次の処理に進む。

【０３８７】

セキュリティモジュール１３と光ディスク記録再生装置１００の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール１３と光

ディスク記録再生装置１００は、セッション鍵Ｋseを生成して共有する。また、セキュリティモジュール１３と光ディスク記録再生装置１００の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール１３と光ディスク記録再生装置１００は、それぞれ相手方が持っているリストのバージョンナンバーのチェックを行う。

【０３８８】

両者のバージョンナンバーが同じである場合、光ディスク記録再生装置１００とセキュリティモジュール１３は、それぞれが保持するリストを用いて相手方のＩＤの検証を行い、互いに相手方が正当であるか否かを検証する。このリストの相互検証の結果、両者において共に正当であると判定された場合には、後段の手順Ｐ２６の処理に進む。また、セキュリティモジュール１３において、光ディスク記録再生装置１００が不正な装置であると判定した場合は、当該プロトコルを終了する。同じく、光ディスク記録再生装置１００において、セキュリティモジュール１３が不正な媒体のものであると判定した場合は、当該プロトコルを終了する。

【０３８９】

一方、セキュリティモジュール１３と光ディスク記録再生装置１００においてそれぞれ相手方が持っているリストのバージョンナンバーのチェックを行った結果、何れか一方の保持しているバージョンよりも他方のバージョンが新しい場合、手順Ｐ２４又はＰ２５として、上記新しいバージョンのリストを相手方に送り、この新しいバージョンのリストを受け取った側では当該新しいバージョンのリストを用いて相手方のＩＤ検証を行うと共に、古いバージョンのリストを更新する。

【０３９０】

その後の手順Ｐ２６以降は、前記図１１、図２９の場合と同様である。

【０３９１】

次に、本発明の第６の実施の形態について説明する。

【０３９２】

第６の実施の形態は、前述の第２，第４の実施の形態で説明したメモリ情報記

録媒体２０のセキュリティモジュール２３の不揮発性メモリ４４と、メモリ記録再生装置２００の不揮発性メモリ２１０に、前記リボケーションリストとレジストレーションリストを格納するようにした例である。当該第６の実施の形態におけるメモリ情報記録媒体２０、メモリ記録再生装置２００の構成は、前記図１２～図１４と同じであるため、それら構成についての説明は省略する。

【０３９３】

図４５～図４８を用いて、第６の実施の形態のメモリ記録再生装置２００がメモリ情報記録媒体２０にデータを記録する手順を説明する。なお、図４５～図４８は、前記第２の実施の形態の図１５～図１８、第４の実施の形態の図３０～図３３と略々同様な図面であり、各手順についても略々同じであるため、以下の説明では、前記図１５～図１８、図３０～図３３とは異なる部分のみ説明する。

【０３９４】

図４５は前記図１５、図３０と略々同様な手順を表しており、手順Ｒ３２として、メモリ記録再生装置２００とセキュリティモジュール２３との間でリボケーションリスト／レジストレーションリストのバージョンナンバーを交換する。

【０３９５】

また、手順Ｒ３３，Ｒ３４では、何れかの一方が他方のリストより新しいリストを持っていた場合、当該新しいリストを持っている方は自分のリストを他方に送る。一方、古いリストを持っている方は、新しいリストを持っている方から、当該新しいリストを送ってもらい、その正当性を検証した後、自分が持つリストを、その送られてきた新しいリストに更新する。

【０３９６】

なお、手順Ｒ３３，Ｒ３４におけるリストの送付は、後の手順Ｒ５におけるデータの記録と順序が前後してもかまわない。つまり、手順Ｒ３５にてデータの記録を行った後に、手順Ｒ３３或いはＲ３４でのリストの送付を行うようにしてもよい。

【０３９７】

次に、図４６には、上記図４５に示した第６の実施の形態のメモリ記録再生装置２００がメモリ情報記録媒体２０にデータを記録するまでの手順の詳細を示し

ており、前記図１６、図３１と略々同様な手順となっている。

【０３９８】

この図４６において、手順Ｒ４２の際のセキュリティモジュール２３は、乱数R_A、乱数R_B、値V_A、リボケーションリストのバージョンナンバー$RevV_A$、レジストレーションリストのバージョンナンバー$RegV_A$からなるビット列にデジタル署名を行いSig_Aを得る。セキュリティモジュール２３は、これらに証明書$Cert_A$を付け、メモリ記録再生装置２００に送る。なお、セキュリティモジュール２３がリボケーションリスト／レジストレーションリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして０を用いる。

【０３９９】

それら$Cert_A$, R_A, R_B, V_A, $RevV_A$, $RegV_A$, Sig_Aを受け取ったメモリ記録再生装置２００は、証明書$Cert_A$、デジタル署名Sig_A、ID_Aの検証を行い、その検証をパスし、さらに、セキュリティモジュール２３から返送されてきた乱数R_Bと先に生成したものとが等しく、且つデジタル署名Sig_Aが正当であると判定されたとき、自己が保持しているリボケーションリスト／レジストレーションリストを用い、メモリ情報記録媒体２０が正当なものであるか否か検証する。この検証の結果、メモリ情報記録媒体２０が不正な媒体であると判定された場合は、、当該プロトコルを終了する。

【０４００】

一方、上記メモリ情報記録媒体２０が正当であると判断された場合、メモリ記録再生装置２００は、手順Ｒ４３として、K_Bの生成と$V_B=K_B \cdot G$の計算を行い、更に、上記乱数R_B、乱数R_A、値V_B、当該装置２００が持つリボケーションリストリストのバージョンナンバー$RevV_B$、レジストレーションリストのバージョンナンバー$RegV_B$からなるビット列にデジタル署名を行ってSig_Bを得る。メモリ記録再生装置２００は、これらに証明書$Cert_B$を付け、セキュリティモジュール２３に送る。なお、メモリ記録再生装置２００がリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして０を用いる。

【０４０１】

上記メモリ記録再生装置２００から$Cert_B$, R_B, R_A, V_B, $RevV_B$, RegV

$_B$，Sig_Bを受け取ると、セキュリティモジュール２３は、証明書$Cert_B$、デジタル署名Sig_B、ID_Bの検証を行い、その検証をパスした時、自己が保持するリボケーションリスト／レジストレーションリストを用い、メモリ記録再生装置２００が正当であるか否か検証する。この検証の結果、メモリ記録再生装置２００が不正な装置であると判定された場合は、当該プロトコルを終了する。

【０４０２】

一方、メモリ記録再生装置２００が正当であると判断された場合、すなわち、セキュリティモジュール２３とメモリ記録再生装置２００の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール２３とメモリ記録再生装置２００はセッション鍵Ｋseを生成して共有する。

【０４０３】

次に、セキュリティモジュール２３とメモリ記録再生装置２００は、それぞれ相手方が持っているリストのバージョンナンバーのチェックを行い、自己の保持しているバージョンよりも新しい場合、手順Ｒ４４又はＲ４５として、その新しいバージョンのリストを相手方に送る。上述のように、相手方から新しいバージョンナンバーのリストが送られてきた方は、当該リスト内に含まれるセンタＴＣの署名ＴＣSigを検証し、その検証をパスしたとき、その新しいリストを用いて自己が保持している古いリストを更新（リストのアップデート）する。

【０４０４】

その後の手順Ｒ４６以降は、前記図１６、図３１の場合と同様である。

【０４０５】

なお、上記リストの伝送は、コンテンツデータの伝送の合間、または終了後に行ってもよい。

【０４０６】

図４７には、前記第２の実施の形態における図１７の手順、第４の実施の形態における図３２の手順を、リボケーションリスト／レジストレーションリストにも適用した例を示している。すなわち、図４７では、先にリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のリストを用いて相手方のＩＤを検証するようにした場合の、データ記録時の手順を示している。

【０４０７】

この図４７において、手順Ｒ５２の際のセキュリティモジュール２３は、乱数R_A、乱数R_B、値V_A、リボケーションリストのバージョンナンバー$RevV_A$、レジストレーションリストのバージョンナンバー$RegV_A$からなるビット列にデジタル署名を行ってSig_Aを得、これらに証明書$Cert_A$を付けてメモリ記録再生装置２００に送る。

【０４０８】

これら$Cert_A$，R_A，R_B，V_A，$RevV_A$，$RegV_A$，Sig_Aを受け取ったメモリ記録再生装置２００は、証明書$Cert_A$、デジタル署名Sig_Aの検証を行い、その検証をパスし、さらに、セキュリティモジュール２３から返送されてきた乱数R_Bと先に生成したものとが等しく、且つデジタル署名Sig_Aが正当であると判定されたとき、手順Ｒ５３として、K_Bを生成し、$V_B=K_B \cdot G$の計算を行い、更に、上記乱数R_B、乱数R_A、値V_B、当該装置２００が持つリボケーションリストのバージョンナンバー$RevV_B$、レジストレーションリストリストのバージョンナンバー$RegV_B$からなるビット列にデジタル署名を行ってSig_Bを得る。メモリ記録再生装置２００は、これらR_B，R_A，V_B，$RegV_B$，$RevV_B$，Sig_Bに証明書$Cert_B$を付け、セキュリティモジュール２３に送る。

【０４０９】

上記メモリ記録再生装置２００から$Cert_B$，R_B，R_A，V_B，$RevV_B$，$RegV_B$，Sig_Bを受け取ると、セキュリティモジュール２３は、証明書$Cert_B$、デジタル署名Sig_Bの検証を行い、その検証をパスした時、次の処理に進む。

【０４１０】

上述のように、セキュリティモジュール２３とメモリ記録再生装置２００の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール２３とメモリ記録再生装置２００は、セッション鍵Ｋseを生成して共有する。

【０４１１】

また、セキュリティモジュール２３とメモリ記録再生装置２００の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール２３とメモリ記録再生装置２００は、それぞれ相手方が持っているリストのバージョン

ナンバーのチェックを行う。

【０４１２】

ここで、両者のバージョンナンバーが同じである場合、メモリ記録再生装置２００とセキュリティモジュール２３は、それぞれが保持するリストを用いて相手方のＩＤの検証を行い、互いに相手方のＩＤがリストに登録されていることを検証する。このリストの相互検証の結果、両者において共にリストに登録されていると判定された場合には、後段の手順Ｒ５６の処理に進む。また、セキュリティモジュール２３において、メモリ記録再生装置２００が不正な装置であると判定された場合は、当該プロトコルを終了する。同じく、メモリ記録再生装置２００において、セキュリティモジュール２３が不正な媒体のものであると判定された場合は、当該プロトコルを終了する。

【０４１３】

一方、セキュリティモジュール２３とメモリ記録再生装置２００においてそれぞれ相手方が持っているリストのバージョンナンバーのチェックを行った結果、何れか一方の保持しているバージョンよりも他方のバージョンが新しい場合、手順Ｒ５４又はＲ５５として、上記新しいバージョンのリストを相手方に送り、この新しいバージョンのリストを受け取った側では当該新しいバージョンのリストを用いて相手方のＩＤ検証を行うと共に、古いバージョンのリストを更新する。

【０４１４】

その後の手順Ｒ５６以降は、前記図１７、図３２の場合と同様である。

【０４１５】

次に、この第６の実施の形態において、メモリ情報記録媒体２０のメモリ部２２へのデータの記録処理については、前述の図１８や図３３と同様の図４８に示すような手順とすることも可能である。

【０４１６】

この図４８において、メモリ記録再生装置２００とセキュリティモジュール２３は、手順Ｒ６２にて相互にリボケーションリスト／レジストレーションリストのバージョンナンバーを交換する。

【０４１７】

また、手順Ｒ６３、Ｒ６４では、リストのバージョンナンバーが古い方を、新しいバージョンナンバーのリストにて更新する。

【０４１８】

手順Ｒ６５以降の処理は、前記図１８、図３３と同様である。

【０４１９】

次に、図４９～図５２を用いて、上記第６の実施の形態のメモリ記録再生装置２００がメモリ情報記録媒体２０のメモリ部２２からデータを再生する手順を説明する。なお、図４９～図５２は、前記第２の実施の形態の図１９～図２２や第４の実施の形態の図３４～図３７と略々同様な図面であり、各手順についても略々同じであるため、以下の説明では、前記図１９～図２２や図３４～図３７とは異なる部分のみ説明する。

【０４２０】

図４９において、メモリ記録再生装置２００とセキュリティモジュール２３は、手順Ｐ３２にて、リボケーションリスト／レジストレーションリストに相手方のＩＤが載せられていないことの確認を互いに行い、自分が持つリストのバージョンナンバーを送り合う。

【０４２１】

また、手順Ｐ３３，Ｐ３４として、メモリ記録再生装置２００とセキュリティモジュール２３は、どちらかが相対的に新しいリストを持っていた場合には、それを他方に送り、送られた方はそれを用いて自分のリストを更新することも同様である。

【０４２２】

その後の手順Ｐ３５以降は、前記図１９、図３４の場合と同様である。

【０４２３】

次に、図５０には、上記図２０に示した第２の実施の形態や図３５に示した第４の実施の形態のメモリ記録再生装置２００がメモリ部２２からデータを再生するまでの手順の詳細を示している。なお、当該図５０の手順は、前記図２０，図３５と略々同様な手順となっている。

【０４２４】

この図５０において、手順Ｐ４２の際のセキュリティモジュール２３は、乱数R_A、乱数R_B、値V_A、リボケーションリストのバージョンナンバー$RevV_A$、レジストレーションリストのバージョンナンバー$RegV_A$からなるビット列にデジタル署名を行いSig_Aを得る。セキュリティモジュール２３は、これらに証明書$Cert_A$を付け、メモリ記録再生装置２００に送る。なお、セキュリティモジュール２３がリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして０を用いる。

【０４２５】

これら$Cert_A$，R_A，R_B，V_A，$RevV_A$，$RegV_A$，Sig_Aを受け取ったメモリ記録再生装置２００は、証明書$Cert_A$、デジタル署名Sig_A、ID_Aの検証を行い、その検証をパスし、さらに、セキュリティモジュール２３から返送されてきた乱数R_Bと先に生成したものとが等しく、且つデジタル署名Sig_Aが正当であると判定されたとき、自己が保持するリストを用い、メモリ情報記録媒体２０が正当であるか否かの検証を行う。この検証の結果、メモリ情報記録媒体２０が不正な媒体であると判定した場合は、当該プロトコルを終了する。

【０４２６】

一方、上記メモリ情報記録媒体２０が正当であると判断した場合、メモリ記録再生装置２００は、手順Ｐ４３として、K_Bの生成と$V_B=K_B \cdot G$の計算を行い、更に、上記乱数R_B、乱数R_A、値V_B、当該装置２００のレジストレーションリストのバージョンナンバー$RevV_B$、レジストレーションリストのバージョンナンバー$RegV_B$からなるビット列にデジタル署名を行ってSig_Bを得る。メモリ記録再生装置２００は、これらに証明書$Cert_B$を付け、セキュリティモジュール２３に送る。なお、メモリ記録再生装置２００がリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして０を用いる。

【０４２７】

上記メモリ記録再生装置２００から$Cert_B$，R_B，R_A，V_B，$RevV_B$，$RegV_B$，Sig_Bを受け取ると、セキュリティモジュール２３は、証明書$Cert_B$、デジタル署名Sig_B、ID_Bの検証を行い、その検証をパスした時、自己が保持するリス

トを用い、メモリ記録再生装置２００が正当であるか否かを検証する。この検証の結果、メモリ記録再生装置２００が不正な装置であると判定した場合は、当該プロトコルを終了する。

【０４２８】

一方、メモリ記録再生装置２００が正当であると判断した場合、すなわち、セキュリティモジュール２３とメモリ記録再生装置２００の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール２３とメモリ記録再生装置２００はセッション鍵Ｋseを生成して共有する。

【０４２９】

次に、セキュリティモジュール２３とメモリ記録再生装置２００は、それぞれ相手方が持っているリボケーションリスト／レジストレーションリストのバージョンナンバーのチェックを行い、自己の保持しているバージョンよりも新しい場合、手順Ｐ４４又はＰ４５として、その新しいバージョンのリストを相手方に送る。上述のように、相手方から新しいバージョンナンバーのリストが送られてきた方は、当該リスト内に含まれるセンタＴＣの署名ＴＣSigを検証し、その検証をパスしたとき、その新しいリストを用いて自己が保持している古いリストを更新する。

【０４３０】

その後の手順Ｐ４６以降は、前記図２０、図３５の場合と同様である。

【０４３１】

なお、上記リストの伝送は、コンテンツデータの伝送の合間、または終了後に行ってもよい。

【０４３２】

図５１には、前記第２の実施の形態における図２１や第４の実施の形態における図３６の手順を、リボケーションリスト／レジストレーションリストにも適用した例を示している。すなわち、図５１は、先にリボケーションリスト／レジストレーションリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のリストを用いて相手方のＩＤを検証するようにした場合の、データ再生時の手順を示している。

【０４３３】

この図５１において、手順Ｐ５２の際のセキュリティモジュール２３は、乱数R_A、乱数R_B、値V_A、リボケーションリストのバージョンナンバー$RevV_A$、レジストレーションリストバージョンナンバー$RegV_A$からなるビット列にデジタル署名を行ってSig_Aを得、これらに証明書$Cert_A$を付けてメモリ記録再生装置２００に送る。

【０４３４】

それらを受け取ったメモリ記録再生装置２００は、証明書$Cert_A$、デジタル署名Sig_Aの検証を行い、その検証をパスし、さらに、セキュリティモジュール２３から返送されてきた乱数R_Bと先に生成したものとが等しく、且つデジタル署名Sig_Aが正当であると判定されたとき、手順Ｐ５３として、K_Bを生成し、$V_B = K_B \cdot G$の計算を行い、更に、上記乱数R_B、乱数R_A、値V_B、当該装置２００が持つリボケーションリストのバージョンナンバー$RevV_B$、レジストレーションリストのバージョンナンバー$RegV_B$からなるビット列にデジタル署名を行ってSig_Bを得る。メモリ記録再生装置２００は、これらに証明書$Cert_B$を付け、セキュリティモジュール２３に送る。

【０４３５】

上記メモリ記録再生装置２００から$Cert_B$, R_B, R_A, V_B, $RevV_B$, $RegV_B$, Sig_Bを受け取ると、セキュリティモジュール２３は、証明書$Cert_B$、デジタル署名Sig_Bの検証を行い、その検証をパスした時、次の処理に進む。

【０４３６】

セキュリティモジュール２３とメモリ記録再生装置２００の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール２３とメモリ記録再生装置２００は、セッション鍵Kseを生成して共有する。また、セキュリティモジュール２３とメモリ記録再生装置２００の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール２３とメモリ記録再生装置２００は、それぞれ相手方が持っているリストのバージョンナンバーのチェックを行う。

【０４３７】

両者のバージョンナンバーが同じである場合、メモリ記録再生装置２００とセキュリティモジュール２３は、それぞれが保持するリストを用いて相手方のＩＤの検証を行い、互いに相手方が正当であるか否かの検証を行う。このンリストの相互検証の結果、両者において共に正当であると判定された場合は、後段の手順Ｐ５６の処理に進む。また、セキュリティモジュール２３において、メモリ記録再生装置２００が不正な装置であると判定した場合は、当該プロトコルを終了する。同じく、メモリ記録再生装置２００において、セキュリティモジュール２３が不正な媒体のものであると判定した場合は、当該プロトコルを終了する。

【０４３８】

一方、セキュリティモジュール２３とメモリ記録再生装置２００においてそれぞれ相手方が持っているリストのバージョンナンバーのチェックを行った結果、何れか一方の保持しているバージョンよりも他方のバージョンが新しい場合、手順Ｐ５４又はＰ５５として、上記新しいバージョンのリストを相手方に送り、この新しいバージョンのリストを受け取った側では当該新しいバージョンのリストを用いて相手方のＩＤ検証を行うと共に、古いバージョンのリストを更新する。

【０４３９】

その後の手順Ｐ５６以降は、前記図２１、図３６の場合と同様である。

【０４４０】

次に、この第６の実施の形態において、メモリ情報記録媒体２０のメモリ部２２からのデータの再生処理については、前述の図２２や図３７と同様の図５２に示すような手順とすることも可能である。

【０４４１】

この図５２において、メモリ記録再生装置２００とセキュリティモジュール２３は、手順Ｐ６２にて相互にリボケーションリスト／レジストレーションリストのバージョンナンバーを交換する。

【０４４２】

また、手順Ｐ６３、Ｐ６４では、リストのバージョンナンバーが古い方を、新しいバージョンナンバーのリストにて更新する。

【０４４３】

手順Ｐ６５以降の処理は、前記図２２、図３７と同様である。

【０４４４】

ところで、上述した第１～第６の実施の形態では、記録再生装置（１００、２００）が不揮発性メモリ（１１０、２１０）を備え、情報記録媒体のセキュリティモジュール（１３、２３）が不揮発性メモリ（３４、４４）備え、これら不揮発性メモリにリボケーションリスト及び／又はレジストレーションリストを格納している例について説明したが、それら記録再生装置と情報記録媒体の何れか一方或いは両方において、リボケーションリスト／レジストレーションリストを格納するための不揮発性メモリを備えていない場合も考えられる。すなわち、リストを格納するための不揮発性メモリを備えることは、コストの上昇に繋がるため、当該不揮発性メモリを備えない記録再生装置や情報記録媒体、或いは、秘密鍵や公開鍵は記憶できるがリストの情報については記憶できるだけの十分な記憶容量を持たない安価な不揮発性メモリしか備えていない記録再生装置や情報記録媒体が存在することが考えられる。

【０４４５】

なお、本発明の各実施の形態では、一つの不揮発性メモリにリストを格納する例を挙げているが、もちろん２以上の不揮発性メモリにリストを格納しても、また一つの不揮発性メモリ内の一部の領域にリストを格納するようにしても良い。さらに、情報記録媒体内に設けられる不揮発性メモリは、セキュリティモジュールの外に配置されるものであってもよい。言い換えると、上述した各実施の形態において、リストを格納するための不揮発性メモリとは、前記暗号化されたコンテンツデータを記録する領域（前記光ディスク１２のデータ記憶領域や、メモリ部２２）以外の記憶領域であって、上記リストを記憶するために特に設けられた記憶領域のことを意味しており、公開鍵や秘密鍵を保持する記憶領域とは異なっている。

【０４４６】

ここで、リボケーションリスト及び／又はレジストレーションリストを十分に格納できる不揮発性メモリを備えるか否かにより、上記情報記録媒体は以下に説

明する第１、第２の媒体タイプに分類することができ、また、上記記録再生装置は、以下の第１、第２の装置タイプに分類することができる。

【０４４７】

第１の媒体タイプは、情報記録媒体が、上記リボケーションリスト及び／又はレジストレーションリストを格納するための不揮発性メモリを備えておらず、これらリストを当該情報記録媒体のコンテンツデータ記録用の領域に格納するようにした場合である。なお、第１の媒体タイプには、上記不揮発性メモリが上記リストを格納するのに十分な記憶容量を有していない場合も含む。

【０４４８】

第２の媒体タイプは、情報記録媒体が上記リボケーションリスト及び／又はレジストレーションリストを格納するための不揮発性メモリを備えている場合である。

【０４４９】

第１の装置タイプは、記録再生装置が、上記リボケーションリスト及び／又はレジストレーションリストを格納するための不揮発性メモリを備えていない場合である。なお、第１の装置タイプには、上記不揮発性メモリが上記リストを格納するのに十分な記憶容量を有していない場合も含む。

【０４５０】

第２の装置タイプは、記録再生装置が、上記リボケーションリスト及び／又はレジストレーションリストを格納するための不揮発性メモリを備えている場合である。

【０４５１】

なお、以下の説明では、上記第１の媒体タイプに相当する光ディスク情報記録媒体をメディアタイプＩＭ１とし、上記第２の媒体タイプに相当する光ディスク情報記録媒体をメディアタイプＩＭ２とし、上記第１の媒体タイプに相当するメモリ情報記録媒体をメディアタイプＩＭ３とし、上記第２の媒体タイプに相当するメモリ情報記録媒体をメディアタイプＩＭ４と呼ぶことにする。さらに、上記第１の装置タイプに相当する光ディスク記録再生装置をデバイスタイプＤｅｖ１とし、上記第２の装置タイプに相当する光ディスク記録再生装置をデバイスタイ

プＤｅｖ２とし、上記第１の装置タイプに相当するメモリ記録再生装置をデバイスタイプＤｅｖ３とし、上記第２の装置タイプに相当するメモリ記録再生装置をデバイスタイプＤｅｖ４とする。

【０４５２】

図５３には、当該メディアタイプＩＭ１に相当する光ディスク情報記録媒体５０の概略構成を示す。この図５３に示すメディアタイプＩＭ１の光ディスク情報記録媒体５０は、図５４に示すように、リストを格納するための不揮発性メモリを持たないセキュリティモジュール５３を備えている。ただし、この図５４に示すようにリストを格納するための不揮発性メモリを持たないセキュリティモジュール５３であっても、秘密鍵、公開鍵証明書、ＩＤ、バージョンナンバーを記憶するためのメモリは必要であり、したがって、当該図５４のセキュリティモジュール５３は、それら秘密鍵、公開鍵証明書、ＩＤ、バージョンナンバーを記憶するための不揮発性の鍵メモリ３６を備えている。なお、図５３、図５４における各部の構成は、前述の図１、図２の例と同じであるため、それらの説明は省略する。

【０４５３】

また、図５５には、上記メディアタイプＩＭ３に相当するメモリ情報記録媒体６０の概略構成を示す。この図５５に示すメディアタイプＩＭ３のメモリ情報記録媒体６０は、図５６に示すように、リストを格納するための不揮発性メモリを持たないセキュリティモジュール６３を備えている。なお、これら図５５、図５６における各部の構成は前述の図１１、図１２の例と同じであるため、それらの説明は省略する。

【０４５４】

以下、上記メディアタイプＩＭ１とデバイスタイプＤｅｖ１の組み合わせ（ＩＭ１，Ｄｅｖ１）、メディアタイプＩＭ１とデバイスタイプＤｅｖ２の組み合わせ（ＩＭ１，Ｄｅｖ２）、メディアタイプＩＭ２とデバイスタイプＤｅｖ１の組み合わせ（ＩＭ２，Ｄｅｖ１）、メディアタイプＩＭ３とデバイスタイプＤｅｖ３の組み合わせ（ＩＭ３，Ｄｅｖ３）、メディアタイプＩＭ３とデバイスタイプＤｅｖ４の組み合わせ（ＩＭ３，Ｄｅｖ４）、メディアタイプＩＭ４とデバイス

タイプＤｅｖ３の組み合わせ（ＩＭ４，Ｄｅｖ３）のそれぞれについて、データ記録時と再生時の手順の説明を行う。なお、メディアタイプＩＭ２とデバイスタイプＤｅｖ２との組み合わせ（ＩＭ２，Ｄｅｖ２）は、前述した第１、第３、第５の実施の形態に相当し、メディアタイプＩＭ４とデバイスタイプＤｅｖ４との組み合わせ（ＩＭ４，Ｄｅｖ４）は前述した第２、第４、第６の実施の形態に相当するため、これらの組み合わせについての説明は省略する。

【０４５５】

なお、以下の説明では、前述した第５、第６の実施の形態のように、リストとしてリボケーションリストとレジストレーションリストの両方を利用可能とした例を挙げて説明しているが、前述の第１～第４の実施の形態のように何れか一方のリストのみ使用する場合であっても良いことは言うまでもない。また、以下の各実施の形態の説明では、先にリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のリストを用いて相手方のＩＤを検証するようにした場合を例に挙げており、前述の第１～第６の実施の形態にて説明した全ての手順に対応する説明は行わないが、以下の各実施の形態においても前記第１～第６の実施の形態にて説明した全ての手順と同様の手順で処理を行うことは可能である。

【０４５６】

先ず、第７の実施の形態として、メディアタイプＩＭ１とデバイスタイプＤｅｖ１の組み合わせ（ＩＭ１，Ｄｅｖ１）から説明する。

【０４５７】

当該第７の実施の形態の組み合わせにおけるシステム構成は、図５７に示すようになる。すなわち、デバイスタイプＤｅｖ１の光ディスク記録再生装置３００はリストを格納するための専用の不揮発性メモリを備えておらず（或いはリストを記憶できる十分な記憶容量を備えていない不揮発性メモリのみ有する）、また、メディアタイプＩＭ１の光ディスク情報記録媒体５０のセキュリティモジュール５３はリストを格納するための不揮発性メモリを備えていない（或いはリストを記憶できる十分な記憶容量を備えていない不揮発性メモリのみ有する）。ただし、この図５７に示すようにリストを格納するための専用の不揮発性メモリを持たない光ディスク記録再生装置３００であっても、秘密鍵、公開鍵証明書、ＩＤ

、バージョンナンバーを記憶するためのメモリは必要であり、したがって、当該図５７の光ディスク記録再生装置３００は、それら秘密鍵、公開鍵証明書、ＩＤ、バージョンナンバーを記憶するための不揮発性の鍵メモリ１１１を備えている。なお、当該図５７における各部の構成は、前述の図３の例と同じであるため、それらの説明は省略する。

【０４５８】

図５８には、当該第７の実施の形態のメディアタイプＩＭ１とデバイスタイプＤｅｖ１の組み合わせ（ＩＭ１，Ｄｅｖ１）の場合に、光ディスク記録再生装置３００が光ディスク情報記録媒体５０にデータを記録する手順を説明する。なお、図５８において前述の各実施の形態の略々同じ手順についての説明は省略し、以下の説明では、それらと異なる部分のみ説明する。

【０４５９】

図５８は前記図３９と略々同様な手順を表しており、手順Ｒ２として、光ディスク記録再生装置３００とセキュリティモジュール５３との間でリボケーションリスト／レジストレーションリストのバージョンナンバーを交換する。ここで、当該第７の実施の形態の場合は、光ディスク記録再生装置３００はリストを持たないため、バージョンナンバー「０」をセキュリティモジュール５３に送り、また、光ディスク情報記録媒体５０は光ディスク１２のコンテンツデータ記録用の領域に記録されているリボケーションリスト／レジストレーションリストのバージョンナンバーを光ディスク記録再生装置３００に送ることになる。このバージョンナンバーは、こうディスク情報記録媒体５０のセキュリティモジュールが覚えておく。

【０４６０】

次に、光ディスク記録再生装置３００は、手順Ｒ１０３として、光ディスク情報記録媒体５０の光ディスク１２のコンテンツデータ記録用の領域に記録されているリボケーションリスト／レジストレーションリストを読み出す。

【０４６１】

当該光ディスク記録再生装置３００は、上記光ディスク情報記録媒体５０から読み出したリストを用いて、当該光ディスク情報記録媒体５０が正当なものであ

るか否か検証し、その検証の結果、当該光ディスク情報記録媒体５０が不正なものであると判定した時は、当該プロトコルを終了する。一方、その光ディスク情報記録媒体５０が正当であると判定した場合は、手順Ｒ１０４として、上記リストをセキュリティモジュール５３に送る。

【０４６２】

セキュリティモジュール５３は、当該リストを用いて、光ディスク記録再生装置３００が正当であるか否かの検証を行い、不正である場合はプロトコルを終了する。

【０４６３】

上記セキュリティモジュール５３が上記リストを用いた検証により正当であると判定した場合、すなわち、光ディスク記録再生装置３００とセキュリティモジュール５３の両者が共に正当であると判定した場合は、後段のデータ暗号化と記録の手順Ｒ５に進むことになる。

【０４６４】

次に、図５９には、上記図５８に示した第７の実施の形態の光ディスク記録再生装置３００が光ディスク情報記録媒体５０にデータを記録するまでの手順の詳細を示しており、前記図４０と略々同様な手順となっている。

【０４６５】

この図５９において、セキュリティモジュール５３は、手順Ｒ１２の際に、乱数R_A、乱数R_B、値V_A、光ディスク１２のデータ記録領域に格納されているリボケーションリストのバージョンナンバー$RevV_A$、レジストレーションリストのバージョンナンバー$RegV_A$からなるビット列に証明書$Cert_A$を付け、光ディスク記録再生装置３００に送る。なお、リボケーションリストのバージョンナンバー$RevV_A$、レジストレーションリストのバージョンナンバー$RegV_A$は、セキュリティモジュールが覚えておく。

【０４６６】

これら$Cert_A$，R_A，R_B，V_A，$RevV_A$，$RegV_A$，Sig_Aを受け取った光ディスク記録再生装置３００は、証明書$Cert_A$、デジタル署名Sig_Aの検証を行い、その検証をパスし、さらに、セキュリティモジュール５３から返送されてきた乱

数R_Bと先に生成したものとが等しく、且つデジタル署名Sig_Aが正当であると判定されたとき、手順Ｒ１３として、乱数R_B、乱数R_A、値V_B、自己がリストを持たないことを示す「０」のバージョンナンバーからなるビット列にデジタル署名を行い、これらR_B，R_A，V_B，０，０，Sig_Bに証明書$Cert_B$を付け、セキュリティモジュール５３に送る。

【０４６７】

上記光ディスク記録再生装置３００から$Cert_B$，R_B，R_A，V_B，０，０，Sig_Bを受け取ると、セキュリティモジュール５３は、証明書$Cert_B$、デジタル署名Sig_Bの検証を行う。この検証をパスしなかった場合は、当該プロトコルを終了する。

【０４６８】

ここで、セキュリティモジュール５３にて当該検証をパスしたとき、すなわち、光ディスク記録再生装置３００とセキュリティモジュール５３の両方で検証をパスしたとき、セキュリティモジュール５３と光ディスク記録再生装置３００はセッション鍵Ｋseを生成して共有する。

【０４６９】

次に、光ディスク記録再生装置３００は、手順Ｒ１１４として、光ディスク１２のデータ記録領域に格納されているリボケーションリスト／レジストレーションリストを読み取り、そのリストのバージョンナンバーが先の手順Ｒ１２で取得したバージョンナンバー（$RevV_A$，$RegV_A$）と等しいこと、及び、当該リストを用いて光ディスク情報記録媒体５０が正当なものであるか否かの検証、当該リスト内に含まれるセンタＴＣの署名ＴＣSigの検証を行う。当該検証において、光ディスク情報記録媒体５０が不正なものであると判定した場合は当該プロトコルを終了する。一方、この検証において正当なものであると判定した場合、光ディスク記録再生装置３００は、手順Ｒ１１５として、そのリストをセキュリティモジュール５３に送る。なお、セキュリティモジュール５３にリストを送るのは、検証の途中であっても良い。

【０４７０】

上記リストを受け取ったセキュリティモジュール５３は、そのリストのバージ

ョンナンバーが前記バージョンナンバー（$RevV_A$，$RegV_A$）と等しいこと、及び、当該リストを用いて光ディスク記録再生装置３００が正当なものであるか否かの検証、当該リスト内に含まれるセンタＴＣの署名ＴＣSigの検証を行う。当該検証において、光ディスク１２が不正なものであると判定した場合は当該プロトコルを終了する。

【０４７１】

一方、この検証において正当なものであると判定した場合、すなわち、光ディスク記録再生装置３００とセキュリティモジュール５３の両方において正当であると判定した場合は、後段の手順Ｒ１６以降のデータ暗号化及び記録の処理に進むことになる。

【０４７２】

次に、図６０には、上記第７の実施の形態の光ディスク記録再生装置３００が光ディスク１２からデータを再生する手順を説明する。なお、図６０の手順は、前記図４３と略々同様な図面であり、各手順についても略々同じであるため、以下の説明では、前記図４３とは異なる部分のみ説明する。

【０４７３】

この図６０において、セキュリティモジュール５３は、手順Ｐ１２の際に、乱数R_A、乱数R_B、値V_A、光ディスク１２のデータ記録領域に記録されているリボケーションリストのバージョンナンバー$RevV_A$、レジストレーションリストのバージョンナンバー$RegV_A$からなるビット列に証明書$Cert_A$を付け、光ディスク記録再生装置３００に送る。

【０４７４】

これら$Cert_A$，R_A，R_B，V_A，$RevV_A$，$RegV_A$，Sig_Aを受け取った光ディスク記録再生装置３００は、証明書$Cert_A$、デジタル署名Sig_Aの検証を行い、その検証をパスし、さらに、セキュリティモジュール５３から返送されてきた乱数R_Bと先に生成したものとが等しく、且つデジタル署名Sig_Aが正当であると判定されたとき、手順Ｐ１３として、乱数R_B、乱数R_A、値V_B、自己がリストを持たないことを示す「０」のバージョンナンバーからなるビット列にデジタル署名を行い、これらR_B，R_A，V_B，０，０，Sig_Bに証明書$Cert_B$を付け、セキュ

リティモジュール５３に送る。

【０４７５】

上記光ディスク記録再生装置３００から$Cert_B$, R_B, R_A, V_B, ０, ０, Sig_Bを受け取ると、セキュリティモジュール５３は、証明書$Cert_B$、デジタル署名Sig_Bの検証を行う。この検証をパスしなかった場合は、当該プロトコルを終了する。

【０４７６】

ここで、セキュリティモジュール５３にて当該検証をパスしたとき、すなわち、光ディスク記録再生装置３００とセキュリティモジュール５３の両方で検証をパスしたとき、セキュリティモジュール５３と光ディスク記録再生装置３００は~~セッション鍵Kseを生成して共有する。~~

【０４７７】

次に、光ディスク記録再生装置３００は、手順Ｐ１１４として、光ディスク１２のデータ記録領域に格納されているリボケーションリスト／レジストレーションリストを読み取り、そのリストのバージョンナンバーが先の手順Ｐ１２で取得したバージョンナンバー（$RevV_A$, $RegV_A$）と等しいこと、及び、当該リストを用いて光ディスク情報記録媒体５０が正当なものであるか否かの検証、当該リスト内に含まれるセンタＴＣの署名ＴＣSigの検証を行う。当該検証において、光ディスク情報記録媒体５０が不正なものであると判定した場合は当該プロトコルを終了する。一方、この検証において正当なものであると判定した場合、光ディスク記録再生装置３００は、手順Ｐ１１５として、そのリストをセキュリティモジュール５３に送る。なお、セキュリティモジュール５３にリストを送るのは、検証の途中であっても良い。

【０４７８】

上記リストを受け取ったセキュリティモジュール５３は、そのリストのバージョンナンバーが前記バージョンナンバー（$RevV_A$, $RegV_A$）と等しいこと、及び、当該リストを用いて光ディスク記録再生装置３００が正当なものであるか否かの検証、当該リスト内に含まれるセンタＴＣの署名ＴＣSigの検証を行う。当該検証において、光ディスク１２が不正なものであると判定した場合は当該プロ

トコルを終了する。

【０４７９】

一方、この検証において正当なものであると判定した場合、すなわち、光ディスク記録再生装置３００とセキュリティモジュール５３の両方において正当であると判定した場合は、後段の手順Ｐ１６以降のデータ再生及び復号処理等に進むことになる。

【０４８０】

次に、第８の実施の形態として、メディアタイプＩＭ１とデバイスタイプＤｅｖ２の組み合わせ（ＩＭ１，Ｄｅｖ２）について説明する。

【０４８１】

当該第８の実施の形態の組み合わせにおけるシステム構成は、図６１に示すようになる。すなわち、デバイスタイプＤｅｖ２の光ディスク記録再生装置１００はリストを格納するための専用の前記不揮発性メモリ１１０を備えており、一方、メディアタイプＩＭ１の光ディスク情報記録媒体５０のセキュリティモジュール５３はリストを格納するための不揮発性メモリを備えていない。なお、当該図６１における各部の構成は、前述の図３の例と同じであるため、それらの説明は省略する。

【０４８２】

図６２には、当該第８の実施の形態のメディアタイプＩＭ１とデバイスタイプＤｅｖ２の組み合わせ（ＩＭ１，Ｄｅｖ２）の場合に、光ディスク記録再生装置１００が光ディスク情報記録媒体５０にデータを記録する手順を説明する。なお、図６２において前述の各実施の形態の略々同じ手順についての説明は省略し、以下の説明では、それらと異なる部分のみ説明する。

【０４８３】

図６２は前記図３９と略々同様な手順を表しており、手順Ｒ２として、光ディスク記録再生装置１００とセキュリティモジュール５３との間でリボケーションリスト／レジストレーションリストのバージョンナンバーを交換する。当該第８の実施の形態の場合、光ディスク記録再生装置１００は、不揮発性メモリ１１０にリボケーションリスト／レジストレーションリストを格納しているため、当該

リストのバージョンナンバーをセキュリティモジュール５３に送り、また、光ディスク情報記録媒体５０は、光ディスク１２のコンテンツデータ記録用の領域に記録されているリボケーションリスト／レジストレーションリストのバージョンナンバーを光ディスク記録再生装置１００に送ることになる。

【０４８４】

ここで、上記手順Ｒ２におけるリストのバージョンナンバーの交換により、光ディスク情報記録媒体５０のリストのバージョンナンバーの方が、光ディスク記録再生装置１００のリストのバージョンナンバーより新しい場合、光ディスク記録再生装置１００は、手順Ｒ１２３として、光ディスク情報記録媒体５０の光ディスク１２のコンテンツデータ記録用の領域に記録されているリボケーションリスト／レジストレーションリストを読み出す。

【０４８５】

当該光ディスク記録再生装置１００は、読み出したリストを用いて、当該光ディスク情報記録媒体５０が正当なものであるか否か検証し、その検証の結果、当該光ディスク情報記録媒体５０が不正なものであると判定した時は、当該プロトコルを終了する。一方、その光ディスク情報記録媒体５０が正当であると判定した場合は、手順Ｒ１２４として、上記光ディスク１２から読み出したリストをセキュリティモジュール５３に送る。また、読み出したリストで自身のものを更新する。このときのセキュリティモジュール５３は、当該リストを用いて、光ディスク記録再生装置１００が正当であるか否かの検証を行い、不正である場合はプロトコルを終了する。

【０４８６】

上記セキュリティモジュール５３が上記リストを用いた検証により正当であると判定した場合、すなわち、光ディスク記録再生装置１００とセキュリティモジュール５３の両者が共に正当であると判定した場合は、後段のデータ暗号化と記録の手順Ｒ５に進むことになる。

【０４８７】

また、上記手順Ｒ２におけるリストのバージョンナンバーの交換により、光ディスク記録再生装置１００が保持するリストのバージョンナンバーが、光ディス

ク情報記録媒体５０のリストのバージョンナンバーより新しいか又は同じである場合、光ディスク記録再生装置１００は、手順Ｒ１２５として、自己が不揮発性メモリ１１０に保持するリストをセキュリティモジュール５３に送る。

【０４８８】

このときのセキュリティモジュール５３は、当該リストを用いて、上記光ディスク記録再生装置１００が正当であるか否かの検証を行い、不正である場合はプロトコルを終了する。

【０４８９】

上記セキュリティモジュール５３が上記リストを用いた検証により正当であると判定した場合、すなわち、光ディスク記録再生装置１００が正当であると判定した場合は、後段のデータ暗号化と記録の手順Ｒ５に進むことになる。

【０４９０】

また、上記手順Ｒ２におけるリストのバージョンナンバーの交換により、光ディスク記録再生装置１００が保持するリストのバージョンナンバーが、光ディスク情報記録媒体５０のリストのバージョンナンバーより新しい場合、光ディスク記録再生装置１００は、手順Ｒ１２６として、自己が不揮発性メモリ１１０に保持するリストを、光ディスク１２のデータ記録領域に記録する。この際、セキュリティモジュールは、そのバージョンナンバーを覚え、以後、使用する。

【０４９１】

次に、図６３には、上記図６２に示した第８の実施の形態の光ディスク記録再生装置１００が光ディスク情報記録媒体５０にデータを記録するまでの手順の詳細を示している。なお、以下の説明では、前記図４１の手順と異なる部分のみ説明する。

【０４９２】

この図６３において、セキュリティモジュール５３は、手順Ｒ２２の際に、乱数R_A、乱数R_B、値V_A、光ディスク１２のデータ記録領域に記録されているリボケーションリストのバージョンナンバー$RevV_A$、レジストレーションリストのバージョンナンバー$RegV_A$からなるビット列に証明書$Cert_A$を付け、光ディスク記録再生装置１００に送る。

【０４９３】

これら$Cert_A$，R_A，R_B，V_A，$RevV_A$，$RegV_A$，Sig_Aを受け取った光ディスク記録再生装置１００は、証明書$Cert_A$、デジタル署名Sig_Aの検証を行い、その検証をパスし、さらに、セキュリティモジュール５３から返送されてきた乱数R_Bと先に生成したものとが等しく、且つデジタル署名Sig_Aが正当であると判定されたとき、手順Ｒ２３として、乱数R_B、乱数R_A、値V_B、自己の不揮発性メモリ１１０に格納しているリストのバージョンナンバー$RevV_B$，$RegV_B$からなるビット列にデジタル署名を行い、これらR_B，R_A，V_B，$RevV_B$，$RegV_B$，Sig_Bに証明書$Cert_B$を付け、セキュリティモジュール５３に送る。

【０４９４】

上記光ディスク記録再生装置１００から$Cert_B$，R_B，R_A，V_B，$RevV_B$，$RegV_B$，Sig_Bを受け取ると、セキュリティモジュール５３は、証明書$Cert_B$、デジタル署名Sig_Bの検証を行う。この検証をパスしなかった場合は、当該プロトコルを終了する。

【０４９５】

ここで、セキュリティモジュール５３にて当該検証をパスしたとき、すなわち、光ディスク記録再生装置１００とセキュリティモジュール５３の両方で検証をパスしたとき、セキュリティモジュール５３と光ディスク記録再生装置１００はセッション鍵Ｋseを生成して共有する。また、セキュリティモジュール５３と光ディスク記録再生装置１００は、それぞれリストのバージョンナンバーの新旧の検証を行う。

【０４９６】

上記リストのバージョンナンバーの新旧検証により、光ディスク情報記録媒体５０のリストのバージョンナンバーの方が、光ディスク記録再生装置１００のリストのバージョンナンバーより新しい場合、光ディスク記録再生装置１００は、手順Ｒ１３４として、光ディスク情報記録媒体５０の光ディスク１２のコンテンツデータ記録用の領域に記録されているリボケーションリスト／レジストレーションリストを読み出り、そのリストのバージョンナンバーが、先に取得したバージョンナンバー（$RevV_A$，$RegV_A$）と等しいこと、及び、当該リストを用いて

光ディスク情報記録媒体５０が正当なものであるか否かの検証、当該リスト内に含まれるセンタＴＣの署名ＴＣSigの検証を行う。当該検証において、光ディスク情報記録媒体５０が不正なものであると判定した場合は当該プロトコルを終了する。一方、この検証において正当なものであると判定した場合、光ディスク記録再生装置３００は、手順Ｒ１３５として、そのリストをセキュリティモジュール５３に送ると共に、当該光ディスク１２から読み取ったリストで自己の不揮発性メモリ１１０内のリストを更新する。なお、セキュリティモジュール５３にリストを送るのは、検証の途中であっても良い。

【０４９７】

上記リストを受け取ったセキュリティモジュール５３は、そのリストのバージョンナンバーが前記バージョンナンバー（$RevV_A$，$RegV_A$）と等しいこと、及び、当該リストを用いて光ディスク記録再生装置１００が正当なものであるか否かの検証、当該リスト内に含まれるセンタＴＣの署名ＴＣSigの検証を行う。当該検証において、光ディスク記録再生装置１００が不正なものであると判定した場合は当該プロトコルを終了する。

【０４９８】

一方、この検証において正当なものであると判定した場合、すなわち、光ディスク記録再生装置１００とセキュリティモジュール５３の両方において正当であると判定した場合は、後段の手順Ｒ２６以降のデータ暗号化及び記録の処理に進むことになる。

【０４９９】

また、上記リストのバージョンナンバーの新旧検証により、光ディスク記録再生装置１００のリストのバージョンナンバーの方が、光ディスク情報記録媒体５０のリストのバージョンナンバーより新しいか同一の場合、光ディスク記録再生装置１００は、自己が保持するリストを用いて、光ディスク情報記録媒体５０が正当か否か検証し、その検証でパスしたとき、手順Ｒ１３６として、当該リストをセキュリティモジュール５３に送る。なお、セキュリティモジュール５３にリストを送るのは、検証の途中であっても良い。

【０５００】

当該リストを受け取ったセキュリティモジュール５３は、そのリストのバージョンナンバーが前記バージョンナンバー（$RevV_B$, $RegV_B$）と等しいこと、及び、当該リストを用いて光ディスク記録再生装置１００が正当なものであるか否かの検証、当該リスト内に含まれるセンタＴＣの署名ＴＣSigの検証を行う。当該検証において、光ディスク記録再生装置１００が不正なものであると判定した場合は当該プロトコルを終了する。

【０５０１】

一方、この検証において正当なものであると判定した場合、すなわち、光ディスク記録再生装置１００とセキュリティモジュール５３の両方において正当であると判定した場合は、後段の手順Ｒ２６以降のデータ暗号化及び記録の処理に進むことになる。

【０５０２】

また、上記リストのバージョンナンバーの新旧検証により、光ディスク記録再生装置１００が保持するリストのバージョンナンバーが、光ディスク情報記録媒体５０のリストのバージョンナンバーより新しい場合、光ディスク記録再生装置１００は、手順Ｒ１３７として、自己が不揮発性メモリ１１０に保持するリストを、光ディスク１２のデータ記録領域に記録する。この際、セキュリティモジュールは、記憶しているバージョンナンバーを更新する。

【０５０３】

次に、図６４には、上記第８の実施の形態の光ディスク記録再生装置１００が光ディスク情報記録媒体５０の光ディスク１２からデータを再生する手順を説明する。なお、図６４の手順は、前記図４４と略々同様であり、以下の説明では、前記図４４とは異なる部分のみ説明する。

【０５０４】

この図６３において、セキュリティモジュール５３は、手順Ｐ２２の際に、乱数R_A、乱数R_B、値V_A、光ディスク１２のデータ記録領域に記録されているリボケーションリストのバージョンナンバー$RevV_A$、レジストレーションリストのバージョンナンバー$RegV_A$からなるビット列に証明書$Cert_A$を付け、光ディ

スク記録再生装置１００に送る。

【０５０５】

これら$Cert_A$，R_A，R_B，V_A，$RevV_A$，$RegV_A$，Sig_Aを受け取った光ディスク記録再生装置１００は、証明書$Cert_A$、デジタル署名Sig_Aの検証を行い、その検証をパスし、さらに、セキュリティモジュール５３から返送されてきた乱数R_Bと先に生成したものとが等しく、且つデジタル署名Sig_Aが正当であると判定されたとき、手順Ｐ２３として、乱数R_B、乱数R_A、値V_B、自己の不揮発性メモリ１１０に格納しているリストのバージョンナンバー$RevV_B$，$RegV_B$からなるビット列にデジタル署名を行い、これらR_B，R_A，V_B，$RevV_B$，$RegV_B$，Sig_Bに証明書$Cert_B$を付け、セキュリティモジュール５３に送る。

【０５０６】

上記光ディスク記録再生装置１００から$Cert_B$，R_B，R_A，V_B，$RevV_B$，$RegV_B$，Sig_Bを受け取ると、セキュリティモジュール５３は、証明書$Cert_B$、デジタル署名Sig_Bの検証を行う。この検証をパスしなかった場合は、当該プロトコルを終了する。

【０５０７】

ここで、セキュリティモジュール５３にて当該検証をパスしたとき、すなわち、光ディスク記録再生装置１００とセキュリティモジュール５３の両方で検証をパスしたとき、セキュリティモジュール５３と光ディスク記録再生装置１００はセッション鍵Ｋseを生成して共有する。また、セキュリティモジュール５３と光ディスク記録再生装置１００は、それぞれリストのバージョンナンバーの新旧の検証を行う。

【０５０８】

上記リストのバージョンナンバーの新旧検証により、光ディスク情報記録媒体５０のリストのバージョンナンバーの方が、光ディスク記録再生装置１００のリストのバージョンナンバーより新しい場合、光ディスク記録再生装置１００は、手順Ｐ１３４として、光ディスク情報記録媒体５０の光ディスク１２のコンテンツデータ記録用の領域に記録されているリボケーションリスト／レジストレーションリストを読み出り、そのリストのバージョンナンバーが、先に取得したバー

ジョンナンバー（$RevV_A$，$RegV_A$）と等しいこと、及び、当該リストを用いて光ディスク情報記録媒体５０が正当なものであるか否かの検証、当該リスト内に含まれるセンタＴＣの署名ＴＣSigの検証を行う。当該検証において、光ディスク情報記録媒体５０が不正なものであると判定した場合は当該プロトコルを終了する。一方、この検証において正当なものであると判定した場合、光ディスク記録再生装置３００は、手順Ｐ１３５として、そのリストをセキュリティモジュール５３に送ると共に、当該光ディスク１２から読み取ったリストで自己の不揮発性メモリ１１０内のリストを更新する。なお、セキュリティモジュール５３にリストを送るのは、検証の途中であっても良い。

【０５０９】

上記リストを受け取ったセキュリティモジュール５３は、そのリストのバージョンナンバーが前記バージョンナンバー（$RevV_A$，$RegV_A$）と等しいこと、及び、当該リストを用いて光ディスク記録再生装置１００が正当なものであるか否かの検証、当該リスト内に含まれるセンタＴＣの署名ＴＣSigの検証を行う。当該検証において、光ディスク記録再生装置１００が不正なものであると判定した場合は当該プロトコルを終了する。

【０５１０】

一方、この検証において正当なものであると判定した場合、すなわち、光ディスク記録再生装置１００とセキュリティモジュール５３の両方において正当であると判定した場合は、後段の手順Ｐ２６以降のデータ再生及び復号の処理に進むことになる。

【０５１１】

また、上記リストのバージョンナンバーの新旧検証により、光ディスク記録再生装置１００のリストのバージョンナンバーの方が、光ディスク情報記録媒体５０のリストのバージョンナンバーより新しいか同一の場合、光ディスク記録再生装置１００は、自己が保持するリストを用いて、光ディスク情報記録媒体５０が正当か否か検証し、その検証でパスしたとき、手順Ｐ１３６として、当該リストをセキュリティモジュール５３に送る。なお、セキュリティモジュール５３にリストを送るのは、検証の途中であっても良い。

【０５１２】

当該リストを受け取ったセキュリティモジュール５３は、そのリストのバージョンナンバーが前記バージョンナンバー（$RevV_B$，$RegV_B$）と等しいこと、及び、当該リストを用いて光ディスク記録再生装置１００が正当なものであるか否かの検証、当該リスト内に含まれるセンタＴＣの署名ＴＣSigの検証を行う。当該検証において、光ディスク記録再生装置１００が不正なものであると判定した場合は当該プロトコルを終了する。

【０５１３】

一方、この検証において正当なものであると判定した場合、すなわち、光ディスク記録再生装置１００とセキュリティモジュール５３の両方において正当であると判定した場合は、後段の手順Ｐ２６以降のデータ再生及び復号のの処理に進むことになる。

【０５１４】

また、上記リストのバージョンナンバーの新旧検証により、光ディスク記録再生装置１００が保持するリストのバージョンナンバーが、光ディスク情報記録媒体５０のリストのバージョンナンバーより新しい場合、光ディスク記録再生装置１００は、手順Ｐ１３７として、自己が不揮発性メモリ１１０に保持するリストを、光ディスク１２のデータ記録領域に記録する。この際、セキュリティモジュールはバージョンナンバーを更新する。

【０５１５】

次に、第９の実施の形態として、メディアタイプＩＭ２とデバイスタイプＤｅｖ１の組み合わせ（ＩＭ２，Ｄｅｖ１）について説明する。

【０５１６】

当該第９の実施の形態の組み合わせにおけるシステム構成は、図６５に示すようになる。すなわち、デバイスタイプＤｅｖ１の光ディスク記録再生装置３００はリストを格納するための専用の前記不揮発性メモリを備えておらず（但し、前述同様に鍵などのメモリは備えている）、メディアタイプＩＭ２の光ディスク情報記録媒体１０のセキュリティモジュール１３はリストを格納するための不揮発性メモリ３４を備えている。なお、当該図６５における各部の構成は、前述の図

３の例と同じであるため、それらの説明は省略する。

【０５１７】

図６６には、当該第９の実施の形態のメディアタイプＩＭ２とデバイスタイプＤｅｖ１の組み合わせ（ＩＭ２，Ｄｅｖ１）の場合に、光ディスク記録再生装置３００が光ディスク情報記録媒体１０にデータを記録する手順を説明する。なお、図６６において前述の各実施の形態の略々同じ手順についての説明は省略し、以下の説明では、それらと異なる部分のみ説明する。

【０５１８】

図６６は前記図３９と略々同様な手順を表しており、手順Ｒ２として、光ディスク記録再生装置３００とセキュリティモジュール１３との間でリボケーションリスト／レジストレーションリストのバージョンナンバーを交換する。当該第９の実施の形態の場合、光ディスク記録再生装置３００は、リボケーションリスト／レジストレーションリストを持たないため、当該リストのバージョンナンバーとして０をセキュリティモジュール１３に送り、光ディスク情報記録媒体１０は、セキュリティモジュール１３内の不揮発性メモリ３４に格納されているリストのバージョンナンバーを光ディスク記録再生装置３００に送ることになる。

【０５１９】

ここで、上記手順Ｒ２におけるリストのバージョンナンバーの交換により、光ディスク記録再生装置３００にはリストが存在しないため、セキュリティモジュール１３は、不揮発性メモリ３４に格納しているリストを用いて光ディスク記録再生装置３００が正当なものであるか否か検証し、その検証の結果、当該光ディスク記録再生装置３００が不正なものであると判定した時は、当該プロトコルを終了する。一方、その光ディスク記録再生装置３００が正当であると判定した場合、セキュリティモジュール１３は、手順Ｒ１４３として、上記不揮発性メモリ３４に格納しているリボケーションリスト／レジストレーションリストを光ディスク記録再生装置３００に送る。

【０５２０】

当該光ディスク記録再生装置３００は、受け取ったリストを用いて、当該光ディスク情報記録媒体１０が正当なものであるか否か検証し、その検証の結果、当

該光ディスク情報記録媒体１０が不正なものであると判定した時は、当該プロトコルを終了する。一方、その光ディスク情報記録媒体１０が正当であると判定した場合は、後段のデータ暗号化と記録の手順Ｒ５に進むことになる。

【０５２１】

次に、図６７には、上記図６６に示した第９の実施の形態の光ディスク記録再生装置３００が光ディスク情報記録媒体１０にデータを記録するまでの手順の詳細を示している。なお、以下の説明では、前記図４３の手順と異なる部分のみ説明する。

【０５２２】

この図６７において、セキュリティモジュール１３は、手順Ｒ１２の際に、乱数R_A、乱数R_B、値V_A、不揮発性メモリ３４から読み出したリボケーションリストのバージョンナンバー$RevV_A$、レジストレーションリストのバージョンナンバー$RegV_A$からなるビット列に証明書$Cert_A$を付け、光ディスク記録再生装置３００に送る。

【０５２３】

これら$Cert_A$，R_A，R_B，V_A，$RevV_A$，$RegV_A$，Sig_Aを受け取った光ディスク記録再生装置３００は、証明書$Cert_A$、デジタル署名Sig_Aの検証を行い、その検証をパスし、さらに、セキュリティモジュール１３から返送されてきた乱数R_Bと先に生成したものとが等しく、且つデジタル署名Sig_Aが正当であると判定されたとき、手順Ｒ１３として、乱数R_B、乱数R_A、値V_B、リストを持たないことを示す「０」のバージョンナンバーからなるビット列にデジタル署名を行い、これらR_B，R_A，V_B，０，０，Sig_Bに証明書$Cert_B$を付け、セキュリティモジュール１３に送る。

【０５２４】

上記光ディスク記録再生装置３００から$Cert_B$，R_B，R_A，V_B，０，０，Sig_Bを受け取ると、セキュリティモジュール１３は、証明書$Cert_B$、デジタル署名Sig_Bの検証を行う。また、セキュリティモジュール１３は、自己が保持するリストを用いて、光ディスク記録再生装置３００が正当であるか否かの検証を行う。これら検証をパスしなかった場合は、当該プロトコルを終了する。

【０５２５】

ここで、セキュリティモジュール１３にて上記検証をパスしたとき、すなわち、光ディスク記録再生装置３００とセキュリティモジュール１３の両方で上記検証をパスしたとき、セキュリティモジュール１３と光ディスク記録再生装置３００はセッション鍵Ｋseを生成して共有する。

【０５２６】

次に、セキュリティモジュール１３は、手順Ｒ１５４として、不揮発性メモリ３４に格納しているリストを光ディスク記録再生装置３００に送る。

【０５２７】

上記リストを受け取った光ディスク記録再生装置３００は、そのリストのバージョンナンバーが前記バージョンナンバー（$RevV_A$，$RegV_A$）と等しいこと、及び、当該リストを用いて光ディスク情報記録媒体１０が正当なものであるか否かの検証、当該リスト内に含まれるセンタＴＣの署名ＴＣSigの検証を行う。当該検証において、光ディスク情報記録媒体１０が不正なものであると判定した場合は当該プロトコルを終了する。

【０５２８】

一方、この検証において正当なものであると判定した場合、すなわち、光ディスク記録再生装置３００とセキュリティモジュール１３の両方において正当であると判定した場合は、後段の手順Ｒ１６以降のデータ暗号化及び記録の処理に進むことになる。

【０５２９】

次に、図６８には、上記第９の実施の形態の光ディスク記録再生装置３００が光ディスク情報記録媒体１０の光ディスク１２からデータを再生する手順を説明する。なお、図６８の手順は、前記図６０と略々同様であり、以下の説明では、前記図６０とは異なる部分のみ説明する。

【０５３０】

この図６８において、セキュリティモジュール１３は、手順Ｐ１２の際に、乱数R_A、乱数R_B、値V_A、不揮発性メモリ３４から読み出したリボケーションリストのバージョンナンバー$RevV_A$、レジストレーションリストのバージョンナ

ンバー$RegV_A$からなるビット列に証明書$Cert_A$を付け、光ディスク記録再生装置３００に送る。

【０５３１】

これら$Cert_A$，R_A，R_B，V_A，$RevV_A$，$RegV_A$，Sig_Aを受け取った光ディスク記録再生装置３００は、証明書$Cert_A$、デジタル署名Sig_Aの検証を行い、その検証をパスし、さらに、セキュリティモジュール１３から返送されてきた乱数R_Bと先に生成したものとが等しく、且つデジタル署名Sig_Aが正当であると判定されたとき、手順Ｐ１３として、乱数R_B、乱数R_A、値V_B、リストを持たないことを示す「０」のバージョンナンバーからなるビット列にデジタル署名を行い、これらR_B，R_A，V_B，０，０，Sig_Bに証明書$Cert_B$を付け、セキュリティモジュール１３に送る。

【０５３２】

上記光ディスク記録再生装置３００から$Cert_B$，R_B，R_A，V_B，０，０，Sig_Bを受け取ると、セキュリティモジュール１３は、証明書$Cert_B$、デジタル署名Sig_Bの検証を行う。また、セキュリティモジュール１３は、自己が保持するリストを用いて、光ディスク記録再生装置３００が正当であるか否かの検証を行う。これら検証をパスしなかった場合は、当該プロトコルを終了する。

【０５３３】

ここで、セキュリティモジュール１３にて上記検証をパスしたとき、すなわち、光ディスク記録再生装置３００とセキュリティモジュール１３の両方で上記検証をパスしたとき、セキュリティモジュール１３と光ディスク記録再生装置３００はセッション鍵Ｋseを生成して共有する。

【０５３４】

次に、セキュリティモジュール１３は、手順Ｐ１５４として、不揮発性メモリ３４に格納しているリストを光ディスク記録再生装置３００に送る。

【０５３５】

上記リストを受け取った光ディスク記録再生装置３００は、そのリストのバージョンナンバーが前記バージョンナンバー（$RevV_A$，$RegV_A$）と等しいこと、及び、当該リストを用いて光ディスク情報記録媒体１０が正当なものであるか否

かの検証、当該リスト内に含まれるセンタＴＣの署名ＴＣSigの検証を行う。当該検証において、光ディスク情報記録媒体１０が不正なものであると判定した場合は当該プロトコルを終了する。

【０５３６】

一方、この検証において正当なものであると判定した場合、すなわち、光ディスク記録再生装置３００とセキュリティモジュール１３の両方において正当であると判定した場合は、後段の手順Ｐ１６以降のデータ再生及び復号の処理に進むことになる。

【０５３７】

次に、第１０の実施の形態として、メディアタイプＩＭ３とデバイスタイプＤｅｖ３の組み合わせ（ＩＭ３，Ｄｅｖ３）から説明する。

【０５３８】

当該第１０の実施の形態の組み合わせにおけるシステム構成は、図６９に示すようになる。すなわち、デバイスタイプＤｅｖ３のメモリ記録再生装置４００はリストを格納するための専用の不揮発性メモリを備えておらず、また、メディアタイプＩＭ３のメモリ情報記録媒体６０のセキュリティモジュール６３はリストを格納するための不揮発性メモリを備えていない。なお、当該図６９における各部の構成は、前述の図１４の例と同じであるため、それらの説明は省略する。

【０５３９】

図７０には、当該第１０の実施の形態のメディアタイプＩＭ３とデバイスタイプＤｅｖ３の組み合わせ（ＩＭ３，Ｄｅｖ３）の場合に、メモリ記録再生装置４００がメモリ情報記録媒体６０にデータを記録する手順を説明する。なお、図７０において前述の各実施の形態の略々同じ手順についての説明は省略し、以下の説明では、それらと異なる部分のみ説明する。

【０５４０】

図７０は前記図４５と略々同様な手順を表しており、手順Ｒ３２として、メモリ記録再生装置４００とセキュリティモジュール６３との間でリボケーションリスト／レジストレーションリストのバージョンナンバーを交換する。ここで、当該第１０の実施の形態の場合は、メモリ記録再生装置４００はリストを持たない

ため、バージョンナンバー０をセキュリティモジュール６３に送り、また、メモリ情報記録媒体６０はメモリ部２２のコンテンツデータ記録用の領域に記録されているリボケーションリスト／レジストレーションリストのバージョンナンバーをメモリ記録再生装置４００に送ることになる。

【０５４１】

次に、セキュリティモジュール６０は、手順Ｒ１６３として、メモリ情報記録媒体６０のメモリ部２２のコンテンツデータ記録用の領域に記録されているリボケーションリスト／レジストレーションリストを読み出す。セキュリティモジュール６０は、このリストを用いて、メモリ記録再生装置４００が正当なものであるか否かの検証を行う。その検証の結果、当該メモリ記録再生装置４００がが不正なものであると判定した時は、当該プロトコルを終了する。一方、そのメモリ記録再生装置４００が正当であると判定した場合は、手順Ｒ１６４として、上記リストをメモリ記録再生装置４００の送る。

【０５４２】

当該メモリ記録再生装置４００は、上記セキュリティモジュール６３から送られたリストを用いて、当該メモリ情報記録媒体６０が正当なものであるか否か検証し、その検証の結果、当該メモリ情報記録媒体６０が不正なものであると判定した時は、当該プロトコルを終了する。

【０５４３】

一方、上記検証において上記メモリ情報記録媒体６０が正当であると判定した場合は、すなわち、メモリ記録再生装置４００とメモリ情報記録媒体６０の両者が共に正当であると判定された場合は、後段のデータ暗号化と記録の手順Ｒ３５に進むことになる。

【０５４４】

次に、図７１には、上記図７０に示した第１０の実施の形態のメモリ記録再生装置４００がメモリ情報記録媒体６０にデータを記録するまでの手順の詳細を示しており、前記図４６と略々同様な手順となっている。

【０５４５】

この図７１において、セキュリティモジュール６３は、手順Ｒ４２の際に、乱

数R_A、乱数R_B、値V_A、メモリ部のデータ記録領域から読み出したリボケーションリストのバージョンナンバー$RevV_A$、レジストレーションリストのバージョンナンバー$RegV_A$からなるビット列に証明書$Cert_A$を付け、メモリ記録再生装置４００に送る。

【０５４６】

これら$Cert_A$，R_A，R_B，V_A，$RevV_A$，$RegV_A$，Sig_Aを受け取ったメモリ記録再生装置４００は、証明書$Cert_A$、デジタル署名Sig_Aの検証を行い、その検証をパスし、さらに、セキュリティモジュール６３から返送されてきた乱数R_Bと先に生成したものとが等しく、且つデジタル署名Sig_Aが正当であると判定されたとき、手順Ｒ４３として、乱数R_B、乱数R_A、値V_B、自己がリストを持たないことを示す「０」のバージョンナンバーからなるビット列にデジタル署名を行い、これらR_B，R_A，V_B，０，０，Sig_Bに証明書$Cert_B$を付け、セキュリティモジュール６３に送る。

【０５４７】

上記メモリ記録再生装置４００から$Cert_B$，R_B，R_A，V_B，０，０，Sig_Bを受け取ると、セキュリティモジュール６３は、証明書$Cert_B$、デジタル署名Sig_Bの検証を行う。この検証をパスしなかった場合は、当該プロトコルを終了する。

【０５４８】

ここで、セキュリティモジュール６３にて当該検証をパスしたとき、すなわち、メモリ記録再生装置４００とセキュリティモジュール６３の両方で検証をパスしたとき、セキュリティモジュール６３とメモリ記録再生装置４００はセッション鍵Ｋseを生成して共有する。

【０５４９】

次に、セキュリティモジュール６３は、手順Ｒ１６４として、メモリ部２２のデータ記録領域に格納されているリボケーションリスト／レジストレーションリストを読み取り、そのリストのバージョンナンバーが先に取得したバージョンナンバー（$RevV_A$，$RegV_A$）と等しいこと、及び、当該リストを用いてメモリ記録再生装置４００が正当なものであるか否かの検証、当該リスト内に含まれるセ

ンタＴＣの署名ＴＣSigの検証を行う。当該検証において、メモリ記録再生装置４００が不正なものであると判定した場合は当該プロトコルを終了する。一方、この検証において正当なものであると判定した場合、セキュリティモジュール６３は、手順Ｒ１６５として、そのリストをメモリ記録再生装置４００に送る。なお、メモリ記録再生装置４００にリストを送るのは、検証の途中であっても良い。

【０５５０】

上記リストを受け取ったメモリ記録再生装置４００は、そのリストのバージョンナンバーが先に取得したバージョンナンバー（$RevV_A$，$RegV_A$）と等しいこと、及び、当該リストを用いてメモリ情報記録媒体６０が正当なものであるか否かの検証、当該リスト内に含まれるセンタＴＣの署名ＴＣSigの検証を行う。当該検証において、メモリ情報記録媒体６０が不正なものであると判定した場合は当該プロトコルを終了する。

【０５５１】

一方、この検証において正当なものであると判定した場合、すなわち、メモリ記録再生装置４００とメモリ情報記録媒体６０の両方において正当であると判定した場合は、後段の手順Ｒ４６以降のデータ暗号化及び記録の処理に進むことになる。

【０５５２】

次に、図７２には、上記第１０の実施の形態のメモリ記録再生装置４００がメモリ情報記録媒体６０のメモリ部２２からデータを再生する手順を説明する。なお、図７２の手順は、前記図５０と略々同様な図面であり、各手順についても略々同じであるため、以下の説明では、前記図５０とは異なる部分のみ説明する。

【０５５３】

この図７２において、セキュリティモジュール６３は、手順Ｐ４２の際に、乱数R_A、乱数R_B、値V_A、メモリ部２２のデータ記録領域から読み出したリボケーションリストのバージョンナンバー$RevV_A$、レジストレーションリストのバージョンナンバー$RegV_A$からなるビット列に証明書$Cert_A$を付け、メモリ記録再生装置４００に送る。

【０５５４】

これら$Cert_A$，R_A，R_B，V_A，$RevV_A$，$RegV_A$，Sig_Aを受け取ったメモリ記録再生装置４００は、証明書$Cert_A$、デジタル署名Sig_Aの検証を行い、その検証をパスし、さらに、セキュリティモジュール６３から返送されてきた乱数R_Bと先に生成したものとが等しく、且つデジタル署名Sig_Aが正当であると判定されたとき、手順Ｐ４３として、乱数R_B、乱数R_A、値V_B、自己がリストを持たないことを示す「０」のバージョンナンバーからなるビット列にデジタル署名を行い、これらR_B，R_A，V_B，０，０，Sig_Bに証明書$Cert_B$を付け、セキュリティモジュール６３に送る。

【０５５５】

上記メモリ記録再生装置４００から$Cert_B$，R_B，R_A，V_B，０，０，Sig_Bを受け取ると、セキュリティモジュール６３は、証明書$Cert_B$、デジタル署名Sig_Bの検証を行う。この検証をパスしなかった場合は、当該プロトコルを終了する。

【０５５６】

ここで、セキュリティモジュール６３にて当該検証をパスしたとき、すなわち、メモリ記録再生装置４００とセキュリティモジュール６３の両方で検証をパスしたとき、セキュリティモジュール６３とメモリ記録再生装置４００はセッション鍵Ｋseを生成して共有する。

【０５５７】

次に、セキュリティモジュール６３は、手順Ｐ１６４として、メモリ部２２のデータ記録領域に格納されているリボケーションリスト／レジストレーションリストを読み取り、そのリストのバージョンナンバーが先に取得したバージョンナンバー（$RevV_A$，$RegV_A$）と等しいこと、及び、当該リストを用いてメモリ記録再生装置４００が正当なものであるか否かの検証、当該リスト内に含まれるセンタＴＣの署名ＴＣSigの検証を行う。当該検証において、メモリ記録再生装置４００が不正なものであると判定した場合は当該プロトコルを終了する。一方、この検証において正当なものであると判定した場合、セキュリティモジュール６３０は、手順Ｐ１６５として、そのリストをメモリ記録再生装置４００に送る。

なお、メモリ記録再生装置４００にリストを送るのは、検証の途中であっても良い。

【０５５８】

上記リストを受け取ったメモリ記録再生装置４００は、そのリストのバージョンナンバーが前記バージョンナンバー（$RevV_A$，$RegV_A$）と等しいこと、及び、当該リストを用いてメモリ情報記録媒体６０が正当なものであるか否かの検証、当該リスト内に含まれるセンタＴＣの署名ＴＣSigの検証を行う。当該検証において、メモリ情報記録媒体６０が不正なものであると判定した場合は当該プロトコルを終了する。

【０５５９】

一方、この検証において正当なものであると判定した場合、すなわち、メモリ記録再生装置４００とセキュリティモジュール６３の両方において正当であると判定した場合は、後段の手順Ｐ４６以降のデータ再生及び復号処理等に進むことになる。

【０５６０】

次に、第１１の実施の形態として、メディアタイプＩＭ３とデバイスタイプＤｅｖ４の組み合わせ（ＩＭ３，Ｄｅｖ４）について説明する。

【０５６１】

当該第１１の実施の形態の組み合わせにおけるシステム構成は、図７３に示すようになる。すなわち、デバイスタイプＤｅｖ４のメモリ記録再生装置２００はリストを格納するための専用の前記不揮発性メモリ２１０を備えており、一方、メディアタイプＩＭ３のメモリ情報記録媒体６０のセキュリティモジュール６３はリストを格納するための不揮発性メモリを備えていない。なお、当該図７３における各部の構成は、前述の図１４の例と同じであるため、それらの説明は省略する。

【０５６２】

図７４には、当該第１１の実施の形態のメディアタイプＩＭ３とデバイスタイプＤｅｖ４の組み合わせ（ＩＭ３，Ｄｅｖ４）の場合に、メモリ記録再生装置２００がメモリ情報記録媒体６０にデータを記録する手順を説明する。なお、図７

４において前述の各実施の形態の略々同じ手順についての説明は省略し、以下の説明では、それらと異なる部分のみ説明する。

【０５６３】

図７４は前記図４５と略々同様な手順を表しており、手順Ｒ３２として、メモリ記録再生装置２００とセキュリティモジュール６３との間でリボケーションリスト／レジストレーションリストのバージョンナンバーを交換する。当該第１１の実施の形態の場合、メモリ記録再生装置２００は、不揮発性メモリ２１０にリボケーションリスト／レジストレーションリストを格納しているため、当該リストのバージョンナンバーをセキュリティモジュール６３に送り、また、メモリ情報記録媒体６０は、メモリ部２２のコンテンツデータ記録用の領域に記録されているリボケーションリスト／レジストレーションリストのバージョンナンバーをメモリ記録再生装置２００に送ることになる。

【０５６４】

ここで、上記手順Ｒ３２におけるリストのバージョンナンバーの交換により、メモリ情報記録媒体６０のメモリ部２２に記録されているリストのバージョンナンバーが、メモリ記録再生装置２００が保持するリストのバージョンナンバーより新しいか又は同じである場合、セキュリティモジュール６３は、手順Ｒ１７３として、メモリ部２２に記録されているリストを読み出す。当該セキュリティモジュール６３は、当該リストを用いて、上記メモリ記録再生装置２００が正当なものであるか否か検証し、その検証の結果、当該メモリ記録再生装置２００が不正なものであると判定した時は、当該プロトコルを終了する。

【０５６５】

一方、そのメモリ記録再生装置２００が正当であると判定した場合は、すなわち、メモリ記録再生装置２００とセキュリティモジュール６３の両者が共に正当であると判定した場合は、後段のデータ暗号化と記録の手順Ｒ３５に進むことになる。また、セキュリティモジュール６３は、手順Ｒ１７４として、上記リストをメモリ記録再生装置２００に送る。

【０５６６】

当該メモリ記録再生装置２００は、上記供給されたリストを用いて、当該メモ

リ情報記録媒体６０が正当なものであるか否か検証し、その検証の結果、当該メモリ情報記録媒体６０が不正なものであると判定した時は、当該プロトコルを終了する。一方、そのメモリ情報記録媒体６０が正当であると判定した場合は、後段のデータ暗号化と記録の手順Ｒ３５に進むことになる。

【０５６７】

また、上記手順Ｒ３２におけるリストのバージョンナンバーの交換により、メモリ記録再生装置２００が保持するリストのバージョンナンバーが、メモリ情報記録媒体６０のメモリ部２２に記録されているリストのバージョンナンバーより新しい場合、メモリ記録再生装置２００は、手順Ｒ１７５として、自己が保持するリストをセキュリティモジュール６３に送る。セキュリティモジュール６３は、当該リストを用いて、上記メモリ記録再生装置２００が正当なものであるか否か検証し、その検証の結果、当該メモリ記録再生装置２００が不正なものであると判定した時は、当該プロトコルを終了する。

【０５６８】

一方、そのメモリ記録再生装置２００が正当であると判定した場合は、セキュリティモジュール６３は、手順Ｒ１７６として、上記メモリ記録再生装置２００から供給されたリストをメモリ部２２のデータ記録領域に記録させると共に、手順Ｒ３５に進む。

【０５６９】

次に、図７５には、上記図７４に示した第１１の実施の形態のメモリ記録再生装置２００がメモリ情報記録媒体６０にデータを記録するまでの手順の詳細を示している。なお、以下の説明では、前記図４７の手順と異なる部分のみ説明する。

【０５７０】

この図７５において、セキュリティモジュール６３は、手順Ｒ５２の際に、乱数R_A、乱数R_B、値V_A、メモリ部２２のデータ記録領域から読み出したリボケーションリストのバージョンナンバー$RevV_A$、レジストレーションリストのバージョンナンバー$RegV_A$からなるビット列に証明書$Cert_A$を付け、メモリ記録再生装置２００に送る。

【０５７１】

これら$Cert_A$，R_A，R_B，V_A，$RevV_A$，$RegV_A$，Sig_Aを受け取ったメモリ記録再生装置２００は、証明書$Cert_A$、デジタル署名Sig_Aの検証を行い、その検証をパスし、さらに、セキュリティモジュール６３から返送されてきた乱数R_Bと先に生成したものとが等しく、且つデジタル署名Sig_Aが正当であると判定されたとき、手順Ｒ５３として、乱数R_B、乱数R_A、値V_B、自己の不揮発性メモリ２１０に格納しているリストのバージョンナンバー$RevV_B$，$RegV_B$からなるビット列にデジタル署名を行い、これらR_B，R_A，V_B，$RevV_B$，$RegV_B$，Sig_Bに証明書$Cert_B$を付け、セキュリティモジュール６３に送る。

【０５７２】

上記メモリ記録再生装置２００から$Cert_B$，R_B，R_A，V_B，$RevV_B$，$RegV_B$，Sig_Bを受け取ると、セキュリティモジュール６３は、証明書$Cert_B$、デジタル署名Sig_Bの検証を行う。この検証をパスしなかった場合は、当該プロトコルを終了する。

【０５７３】

ここで、セキュリティモジュール６３にて当該検証をパスしたとき、すなわち、メモリ記録再生装置２００とセキュリティモジュール６３の両方で検証をパスしたとき、セキュリティモジュール６３とメモリ記録再生装置２００はセッション鍵Ｋseを生成して共有する。

【０５７４】

また、セキュリティモジュール６３とメモリ記録再生装置２００の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール６３とメモリ記録再生装置２００は、それぞれリストのバージョンナンバーのチェックを行う。

【０５７５】

ここで、両者のバージョンナンバーが同じである場合、セキュリティモジュール６３は、手順Ｒ１８４として、メモリ部２２からリストを読み出し、そのリストのバージョンナンバーが先に取得したバージョンナンバー（$RevV_A$，$RegV_A$）と等しいこと、及び、当該リストを用いてメモリ記録再生装置２００が正当な

ものであるか否かの検証、当該リスト内に含まれるセンタＴＣの署名ＴＣSigの検証を行う。当該検証において、メモリ記録再生装置２００が不正なものであると判定した場合は当該プロトコルを終了する。また、この時のメモリ記録再生装置２００は、自己が保持するリストを用いて、メモリ情報記録媒体６０が正当であるか否かの検証を行い、不正なものであると判定したときは当該プロトコルを終了し、これらセキュリティモジュール６３及びメモリ記録再生装置２００において、共に正当であると判定した時は、その後の手順Ｒ５６以降に進むことになる。

【０５７６】

また、両者のバージョンナンバーの検証を行った結果、メモリ情報記録媒体６０のメモリ部２２が保持するリストのバージョンナンバーが、メモリ記録再生装置２００が保持するリストのバージョンナンバーより新しい場合、セキュリティモジュール６３は、手順Ｒ１８５として、メモリ部２２からリストを読み出し、そのリストのバージョンナンバーが先に取得したバージョンナンバー（$RevV_A$，$RegV_A$）と等しいこと、及び、当該リストを用いてメモリ記録再生装置２００が正当なものであるか否かの検証、当該リスト内に含まれるセンタＴＣの署名ＴＣSigの検証を行う。当該検証において、メモリ記録再生装置２００が不正なものであると判定した場合は当該プロトコルを終了する。一方、メモリ記録再生装置２００が正当であると判定した場合は、手順Ｒ１８６として、上記リストをメモリ記録再生装置２００の送る。

【０５７７】

メモリ記録再生装置２００は、当該リストを受け取ると、そのリストのバージョンナンバーが先に取得したバージョンナンバー（$RevV_A$，$RegV_A$）と等しいこと、及び、当該リストを用いてメモリ情報記録媒体６０が正当なものであるか否かの検証、当該リスト内に含まれるセンタＴＣの署名ＴＣSigの検証を行う。当該検証において、メモリ情報記録媒体６０が不正なものであると判定した場合は当該プロトコルを終了する。一方、メモリ情報記録媒体６０が正当であると判定した場合は、その後の手順Ｒ５６以降に進むことになる。

【０５７８】

また、両者のバージョンナンバーの検証を行った結果、メモリ記録再生装置２００が保持するリストのバージョンナンバーが、メモリ情報記録媒体６０のメモリ部２２が保持するリストのバージョンナンバーより新しい場合、メモリ記録再生装置２００は、当該リストを用いてメモリ情報記録媒体６０が正当なものであるか否かを検証し、当該検証において、メモリ情報記録媒体６０が不正なものであると判定した場合は当該プロトコルを終了する。一方、メモリ情報記録媒体６０が正当であると判定した場合は、手順Ｒ１８７として、上記リストをセキュリティモジュール６３に送る。

【０５７９】

セキュリティモジュール６３は、当該リストを受け取ると、そのリストのバージョンナンバーが先に取得したバージョンナンバー（$RevV_B$, $RegV_B$）と等しいこと、及び、当該リストを用いてメモリ記録再生装置２００が正当なものであるか否かの検証、当該リスト内に含まれるセンタＴＣの署名ＴＣSigの検証を行う。当該検証において、メモリ記録再生装置２００が不正なものであると判定した場合は当該プロトコルを終了する。一方、メモリ記録再生装置２００が正当であると判定した場合は、手順Ｒ１８８として、上記リストをメモリ部２２に書き込んで更新し、その後の手順Ｒ５６以降に進むことになる。なお、リストの更新と手順Ｒ５６以降の処理は前後してもかまわない。これらのメディアタイプＩＭ３では、メモリに格納されているリストのバージョンをプロトコル中で読み出すようにしているが、メモリ上でのリストの改ざんを防止するために、バージョンナンバーをセキュリティモジュールが記憶しておくことが望ましい。

【０５８０】

次に、図７６には、上記第１１の実施の形態のメモリ記録再生装置２００がメモリ情報記録媒体６０のメモリ部２２からデータを再生する手順を説明する。なお、図７６の手順は、前記図５１と略々同様であり、以下の説明では、前記図５１とは異なる部分のみ説明する。

【０５８１】

この図７６において、セキュリティモジュール６３は、手順Ｐ５２の際に、乱

数R_A、乱数R_B、値V_A、メモリ部２２のデータ記録領域から読み出したリボケーションリストのバージョンナンバー$RevV_A$、レジストレーションリストのバージョンナンバー$RegV_A$からなるビット列に証明書$Cert_A$を付け、メモリ記録再生装置２００に送る。

【０５８２】

これら$Cert_A$, R_A, R_B, V_A, $RevV_A$, $RegV_A$, Sig_Aを受け取ったメモリ記録再生装置２００は、証明書$Cert_A$、デジタル署名Sig_Aの検証を行い、その検証をパスし、さらに、セキュリティモジュール６３から返送されてきた乱数R_Bと先に生成したものとが等しく、且つデジタル署名Sig_Aが正当であると判定されたとき、手順Ｐ５３として、乱数R_B、乱数R_A、値V_B、自己の不揮発性メモリ２１０に格納しているリストのバージョンナンバー$RevV_B$, $RegV_B$からなるビット列にデジタル署名を行い、これらR_B, R_A, V_B, $RevV_B$, $RegV_B$, Sig_Bに証明書$Cert_B$を付け、セキュリティモジュール６３に送る。

【０５８３】

上記メモリ記録再生装置２００から$Cert_B$, R_B, R_A, V_B, $RevV_B$, $RegV_B$, Sig_Bを受け取ると、セキュリティモジュール６３は、証明書$Cert_B$、デジタル署名Sig_Bの検証を行う。この検証をパスしなかった場合は、当該プロトコルを終了する。

【０５８４】

ここで、セキュリティモジュール６３にて当該検証をパスしたとき、すなわち、メモリ記録再生装置２００とセキュリティモジュール６３の両方で検証をパスしたとき、セキュリティモジュール６３とメモリ記録再生装置２００はセッション鍵Kseを生成して共有する。

【０５８５】

また、セキュリティモジュール６３とメモリ記録再生装置２００の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール６３とメモリ記録再生装置２００は、それぞれリストのバージョンナンバーのチェックを行う。

【０５８６】

ここで、両者のバージョンナンバーが同じである場合、セキュリティモジュール６３は、手順Ｐ１８４として、メモリ部２２からリストを読み出し、そのリストのバージョンナンバーが先に取得したバージョンナンバー（$RevV_A$，$RegV_A$）と等しいこと、及び、当該リストを用いてメモリ記録再生装置２００が正当なものであるか否かの検証、当該リスト内に含まれるセンタＴＣの署名ＴＣSigの検証を行う。当該検証において、メモリ記録再生装置２００が不正なものであると判定した場合は当該プロトコルを終了する。また、この時のメモリ記録再生装置２００は、自己が保持するリストを用いて、メモリ情報記録媒体６０が正当であるか否かの検証を行い、不正なものであると判定したときは当該プロトコルを終了し、これらセキュリティモジュール６３及びメモリ記録再生装置２００において、共に正当であると判定した時は、その後の手順Ｒ５６以降に進むことになる。

【０５８７】

また、両者のバージョンナンバーの検証を行った結果、メモリ情報記録媒体６０のメモリ部２２が保持するリストのバージョンナンバーが、メモリ記録再生装置２００が保持するリストのバージョンナンバーより新しい場合、セキュリティモジュール６３は、手順Ｐ１８５として、メモリ部２２からリストを読み出し、そのリストのバージョンナンバーが先に取得したバージョンナンバー（$RevV_A$，$RegV_A$）と等しいこと、及び、当該リストを用いてメモリ記録再生装置２００が正当なものであるか否かの検証、当該リスト内に含まれるセンタＴＣの署名ＴＣSigの検証を行う。当該検証において、メモリ記録再生装置２００が不正なものであると判定した場合は当該プロトコルを終了する。一方、メモリ記録再生装置２００が正当であると判定した場合は、手順Ｐ１８６として、上記リストをメモリ記録再生装置２００の送る。

【０５８８】

メモリ記録再生装置２００は、当該リストを受け取ると、そのリストのバージョンナンバーが先に取得したバージョンナンバー（$RevV_A$，$RegV_A$）と等しいこと、及び、当該リストを用いてメモリ情報記録媒体６０が正当なものであるか

否かの検証、当該リスト内に含まれるセンタＴＣの署名ＴＣSigの検証を行う。当該検証において、メモリ情報記録媒体６０が不正なものであると判定した場合は当該プロトコルを終了する。一方、メモリ情報記録媒体６０が正当であると判定した場合は、その後の手順Ｐ５６以降に進むことになる。

【０５８９】

また、両者のバージョンナンバーの検証を行った結果、メモリ記録再生装置２００が保持するリストのバージョンナンバーが、メモリ情報記録媒体６０のメモリ部２２が保持するリストのバージョンナンバーより新しい場合、メモリ記録再生装置２００は、当該リストを用いてメモリ情報記録媒体６０が正当なものであるか否かを検証し、当該検証において、メモリ情報記録媒体６０が不正なものであると判定した場合は当該プロトコルを終了する。一方、メモリ情報記録媒体６０が正当であると判定した場合は、手順Ｐ１８７として、上記リストをセキュリティモジュール６３に送る。

【０５９０】

セキュリティモジュール６３は、当該リストを受け取ると、そのリストのバージョンナンバーが先に取得したバージョンナンバー（$RevV_B$，$RegV_B$）と等しいこいと、及び、当該リストを用いてメモリ記録再生装置２００が正当なものであるか否かの検証、当該リスト内に含まれるセンタＴＣの署名ＴＣSigの検証を行う。当該検証において、メモリ記録再生装置２００が不正なものであると判定した場合は当該プロトコルを終了する。一方、メモリ記録再生装置２００が正当であると判定した場合は、手順Ｐ１８８として、上記リストをメモリ部２２に書き込んで更新し、その後の手順Ｐ５６以降に進むことになる。なお、リストの更新と手順Ｐ５６以降の処理は前後してもかまわない。

【０５９１】

次に、第１２の実施の形態として、メディアタイプＩＭ４とデバイスタイプＤｅｖ３の組み合わせ（ＩＭ４，Ｄｅｖ３）について説明する。

【０５９２】

当該第１２の実施の形態の組み合わせにおけるシステム構成は、図７７に示すようになる。すなわち、デバイスタイプＤｅｖ３のメモリ記録再生装置４００は

リストを格納するための専用の前記不揮発性メモリを備えておらず、一方、メディアタイプＩＭ４のメモリ情報記録媒体２０のセキュリティモジュール２３はリストを格納するための不揮発性メモリ４３を備えている。なお、当該図７７における各部の構成は、前述の図１４の例と同じであるため、それらの説明は省略する。

【０５９３】

図７８には、当該第１２の実施の形態のメディアタイプＩＭ４とデバイスタイプＤｅｖ３の組み合わせ（ＩＭ４，Ｄｅｖ３）の場合に、メモリ記録再生装置４００がメモリ情報記録媒体１０にデータを記録する手順を説明する。なお、図７８において前述の各実施の形態の略々同じ手順についての説明は省略し、以下の説明では、それらと異なる部分のみ説明する。

【０５９４】

図７８は前記図４５と略々同様な手順を表しており、手順Ｒ３２として、メモリ記録再生装置４００とセキュリティモジュール２３との間でリボケーションリスト／レジストレーションリストのバージョンナンバーを交換する。当該第１２の実施の形態の場合、メモリ記録再生装置２００は、リボケーションリスト／レジストレーションリストを持たないため、当該リストのバージョンナンバーとして「０」をセキュリティモジュール２３に送り、メモリ情報記録媒体２０は、セキュリティモジュール２３内の不揮発性メモリ４４に格納されているリストのバージョンナンバーをメモリ記録再生装置４００に送ることになる。

【０５９５】

ここで、上記手順Ｒ３２におけるリストのバージョンナンバーの交換により、メモリ記録再生装置４００にはリストが存在しないため、セキュリティモジュール２３は、不揮発性メモリ４４に格納しているリストを用いてメモリ記録再生装置４００が正当なものであるか否か検証し、その検証の結果、当該メモリ記録再生装置４００が不正なものであると判定した時は、当該プロトコルを終了する。一方、そのメモリ記録再生装置４００が正当であると判定した場合、セキュリティモジュール２３は、手順Ｒ１９３として、上記不揮発性メモリ４４に格納しているリボケーションリスト／レジストレーションリストをメモリ記録再生装置４

００に送る。

【０５９６】

当該メモリ記録再生装置４００は、受け取ったリストを用いて、当該メモリ情報記録媒体２０が正当なものであるか否か検証し、その検証の結果、当該メモリ情報記録媒体２０が不正なものであると判定した時は、当該プロトコルを終了する。一方、そのメモリ情報記録媒体２０が正当であると判定した場合は、後段のデータ暗号化と記録の手順Ｒ３５に進むことになる。

【０５９７】

次に、図７９には、上記図７８に示した第１２の実施の形態のメモリ記録再生装置４００がメモリ情報記録媒体２０にデータを記録するまでの手順の詳細を示している。なお、以下の説明では、前記図４６の手順と異なる部分のみ説明する。

【０５９８】

この図７９において、セキュリティモジュール２３は、手順Ｒ４２の際に、乱数R_A、乱数R_B、値V_A、不揮発性メモリ４４から読み出したリボケーションリストのバージョンナンバー$RevV_A$、レジストレーションリストのバージョンナンバー$RegV_A$からなるビット列に証明書$Cert_A$を付け、メモリ記録再生装置４００に送る。

【０５９９】

これら$Cert_A$，R_A，R_B，V_A，$RevV_A$，$RegV_A$，Sig_Aを受け取ったメモリ記録再生装置４００は、証明書$Cert_A$、デジタル署名Sig_Aの検証を行い、その検証をパスし、さらに、セキュリティモジュール２３から返送されてきた乱数R_Bと先に生成したものとが等しく、且つデジタル署名Sig_Aが正当であると判定されたとき、手順Ｒ４３として、乱数R_B、乱数R_A、値V_B、リストを持たないことを示す「０」のバージョンナンバーからなるビット列にデジタル署名を行い、これらR_B，R_A，V_B，０，０，Sig_Bに証明書$Cert_B$を付け、セキュリティモジュール２３に送る。

【０６００】

上記メモリ記録再生装置４００から$Cert_B$，R_B，R_A，V_B，０，０，Sig_Bを

受け取ると、セキュリティモジュール２３は、証明書$Cert_B$、デジタル署名Sig_Bの検証を行う。また、セキュリティモジュール２３は、自己が保持するリストを用いて、メモリ記録再生装置４００が正当であるか否かの検証を行う。これら検証をパスしなかった場合は、当該プロトコルを終了する。

【０６０１】

ここで、セキュリティモジュール２３にて上記検証をパスしたとき、すなわち、メモリ記録再生装置４００とセキュリティモジュール２３の両方で上記検証をパスしたとき、セキュリティモジュール２３とメモリ記録再生装置４００はセッション鍵Kseを生成して共有する。

【０６０２】

次に、セキュリティモジュール２３は、手順Ｒ２０４として、不揮発性メモリ４４に格納しているリストをメモリ記録再生装置４００に送る。

【０６０３】

上記リストを受け取ったメモリ記録再生装置４００は、そのリストのバージョンナンバーが前記バージョンナンバー（$RevV_A$, $RegV_A$）と等しいこと、及び、当該リストを用いてメモリ情報記録媒体２０が正当なものであるか否かの検証、当該リスト内に含まれるセンタＴＣの署名ＴＣSigの検証を行う。当該検証において、メモリ情報記録媒体２０が不正なものであると判定した場合は当該プロトコルを終了する。

【０６０４】

一方、この検証において正当なものであると判定した場合、すなわち、メモリ記録再生装置４００とセキュリティモジュール２３の両方において正当であると判定した場合は、後段の手順Ｒ４６以降のデータ暗号化及び記録の処理に進むことになる。

【０６０５】

次に、図８０には、上記第１２の実施の形態のメモリ記録再生装置４００がメモリ情報記録媒体２０のメモリ部２２からデータを再生する手順を説明する。なお、図８０の手順は、前記図５０と略々同様であり、以下の説明では、前記図５０とは異なる部分のみ説明する。

【０６０６】

この図８０において、セキュリティモジュール２３は、手順Ｐ４２の際に、乱数R_A、乱数R_B、値V_A、不揮発性メモリ４４から読み出したリボケーションリストのバージョンナンバー$RevV_A$、レジストレーションリストのバージョンナンバー$RegV_A$からなるビット列に証明書$Cert_A$を付け、メモリ記録再生装置４００に送る。

【０６０７】

これら$Cert_A$，R_A，R_B，V_A，$RevV_A$，$RegV_A$，Sig_Aを受け取ったメモリ記録再生装置４００は、証明書$Cert_A$、デジタル署名Sig_Aの検証を行い、その検証をパスし、さらに、セキュリティモジュール２３から返送されてきた乱数R_Bと先に生成したものとが等しく、且つデジタル署名Sig_Aが正当であると判定されたとき、手順Ｐ４３として、乱数R_B、乱数R_A、値V_B、リストを持たないことを示す「０」のバージョンナンバーからなるビット列にデジタル署名を行い、これらR_B，R_A，V_B，０，０，Sig_Bに証明書$Cert_B$を付け、セキュリティモジュール２３に送る。

【０６０８】

上記メモリ記録再生装置４００から$Cert_B$，R_B，R_A，V_B，０，０，Sig_Bを受け取ると、セキュリティモジュール２３は、証明書$Cert_B$、デジタル署名Sig_Bの検証を行う。また、セキュリティモジュール２３は、自己が保持するリストを用いて、メモリ記録再生装置４００が正当であるか否かの検証を行う。これら検証をパスしなかった場合は、当該プロトコルを終了する。

【０６０９】

ここで、セキュリティモジュール２３にて上記検証をパスしたとき、すなわち、メモリ記録再生装置４００とセキュリティモジュール２３の両方で上記検証をパスしたとき、セキュリティモジュール２３とメモリ記録再生装置４００はセッション鍵Ksesを生成して共有する。

【０６１０】

次に、セキュリティモジュール２３は、手順Ｐ２０４として、不揮発性メモリ４４に格納しているリストをメモリ記録再生装置４００に送る。

【０６１１】

上記リストを受け取ったメモリ記録再生装置４００は、そのリストのバージョンナンバーが前記バージョンナンバー（$RevV_A$，$RegV_A$）と等しいこと、及び、当該リストを用いてメモリ情報記録媒体２０が正当なものであるか否かの検証、当該リスト内に含まれるセンタＴＣの署名ＴＣSigの検証を行う。当該検証において、メモリ情報記録媒体２０が不正なものであると判定した場合は当該プロトコルを終了する。

【０６１２】

一方、この検証において正当なものであると判定した場合、すなわち、メモリ記録再生装置４００とセキュリティモジュール２３の両方において正当であると判定した場合は、後段の手順Ｐ１６以降のデータ再生及び復号の処理に進むことになる。

【０６１３】

次に、図８１～図８７のフローチャートを用いて、本発明の各実施の形態のセキュリティモジュールと記録再生装置が、それぞれタイプ別に行う処理の流れを説明する。なお、以下の説明では、リボケーションリスト／レジストレーションリストの両方を用いた場合を例に挙げている。

【０６１４】

図８１には、前記メディアタイプＩＭ１に相当する光ディスク情報記録媒体５０のセキュリティモジュール５３における処理の流れを示す。

【０６１５】

この図８１において、セキュリティモジュール５３は、ステップＳ１として、前述したように、光ディスク記録再生装置が発生した乱数R_Bの受信と、前記$V_A = K_A \cdot G$の計算、乱数R_Aの発生、デジタル署名を行いSig_A計算、$Cert_A$，R_A，R_B，V_A，$RevV_A$，$RegV_A$，Sig_Aを光ディスク記録再生装置に送信する。

【０６１６】

次に、セキュリティモジュール５３は、ステップＳ２として、光ディスク記録再生装置から送信されてきた$Cert_B$，R_B，R_A，V_B，$RevV_B$，$RegV_B$，Sig_B受信、$Cert_B$の検証、Sig_Bの検証、セッション鍵Ｋseの計算を行う。

【０６１７】

次に、セキュリティモジュール５３は、ステップＳ３として、例えばリストのバージョンナンバーが「０」か否かにより、相手方の光ディスク記録再生装置のデバイスタイプを判定する。このステップＳ３の判定において、例えばリストのバージョンナンバーが「０」となっており、前記デバイスタイプＤｅｖ１（すなわち前記光ディスク記録再生装置３００）であると判定した場合、セキュリティモジュール５３の処理は、ステップＳ４に進む。一方、ステップＳ３の判定において、リストのバージョンナンバーが「０」でなく、前記デバイスタイプＤｅｖ２（すなわち前記光ディスク記録再生装置１００）であると判定した場合、セキュリティモジュール５３の処理は、ステップＳ５に進む。

【０６１８】

ステップＳ４の処理に進むと、セキュリティモジュール５３は、光ディスク１２のデータ記録領域からリボケーションリスト／レジストレーションリストを読み取り、そのバージョンナンバー（$RevV_A$，$RegV_A$）の検証と、そのリストを用いた光ディスク記録再生装置（デバイスタイプＤｅｖ１の装置３００）のＩＤ$_B$の検証と、センタＴＣの署名ＴＣSigの検証を行った後、ステップＳ８に進む。

【０６１９】

また、ステップＳ５の処理に進むと、セキュリティモジュール５３は、光ディスク１２のデータ記録領域に記録されているリボケーションリスト／レジストレーションリストのバージョンが、デバイスタイプＤｅｖ２の光ディスク記録再生装置１００の保持するリストのバージョンナンバーよりも大きい（Ａ＞Ｂ）か、或いはそれ以下（Ａ≦Ｂ）であるのかの判定を行う。このステップＳ５の判定において、Ａ＞Ｂであると判定した場合、セキュリティモジュール５３の処理はステップＳ６に進み、一方、Ａ≦Ｂであると判定した場合、セキュリティモジュール５３の処理はステップＳ７に進む。

【０６２０】

ステップＳ６の処理に進むと、セキュリティモジュール５３は、光ディスク１２のデータ記録領域からリボケーションリスト／レジストレーションリストを読み取り、そのバージョンナンバー（$RevV_A$，$RegV_A$）の検証と、そのリストを

用いた光ディスク記録再生装置１００のＩＤ$_B$の検証と、センタＴＣの署名ＴＣＳigの検証を行った後、ステップＳ８に進む。

【０６２１】

また、ステップＳ７の処理に進むと、セキュリティモジュール５３は、光ディスク記録再生装置１００が保持するリボケーションリスト／レジストレーションリストを受け取り、そのバージョンナンバー（ＲｅｖV_B，ＲｅｇV_B）の検証と、そのリストを用いた光ディスク記録再生装置１００のＩＤ$_B$の検証と、センタＴＣの署名ＴＣSigの検証を行った後、ステップＳ８に進む。

【０６２２】

ステップＳ８の処理に進むと、セキュリティモジュール５３は、光ディスク記録再生装置から記録又は再生の何れの処理が要求されているのか判定する。

【０６２３】

当該ステップＳ８にて記録の処理が要求されていると判定した場合、セキュリティモジュール５３は、ステップＳ９の処理として、光ディスク記録再生装置がセッション鍵Ｋseにて暗号鍵Ｋcoを暗号化した値Ｅnc（Kse，Kco）を受信して復号し、次に、その復号により得られた暗号鍵Ｋcoを自己が保持するストレージ鍵Ｋstで暗号化した値Ｅnc（Kst，Kco）を生成して光ディスク記録再生装置に送信する。その後、光ディスク記録再生装置において上記暗号鍵Ｋcoにて暗号化されたコンテンツデータＥnc（Kse，Kco）が、光ディスク１２に記録されることになる。

【０６２４】

一方、ステップＳ８にて再生の処理が要求されていると判定した場合、セキュリティモジュール５３は、ステップＳ１０の処理として、ストレージ鍵Ｋstにて暗号鍵Ｋcoが暗号化され例えば光ディスク１２のデータ記録領域等に記録されている値Ｅnc（Kst，Kco）を読み出して復号し、その復号により得られた暗号鍵Ｋcoをセッション鍵Ｋseにて暗号化した値Ｅnc（Kse，Kco）を生成して光ディスク記録再生装置に送信する。その後、上記暗号鍵Ｋcoにて暗号化されているコンテンツデータＥnc（Kse，Kco）は、光ディスク１２から再生されて光ディスク記録再生装置に送られることになる。

【０６２５】

図８２には、前記メディアタイプＩＭ２に相当する光ディスク情報記録媒体１０のセキュリティモジュール１３における処理の流れを示す。

【０６２６】

この図８２において、セキュリティモジュール１３は、ステップＳ１１として、前述したように、光ディスク記録再生装置が発生した乱数R_Bの受信と、前記$V_A = K_A \cdot G$の計算、乱数R_Aの発生、デジタル署名を行いSig_A計算、$Cert_A$, R_A, R_B, V_A, $RevV_A$, $RegV_A$, Sig_Aを光ディスク記録再生装置に送信する。

【０６２７】

次に、セキュリティモジュール１３は、ステップＳ１２として、光ディスク記録再生装置から送信されてきた$Cert_B$, R_B, R_A, V_B, $RevV_B$, $RegV_B$, Sig_B受信、$Cert_B$の検証、Sig_Bの検証、セッション鍵Kseの計算を行う。

【０６２８】

次に、セキュリティモジュール１３は、ステップＳ１３として、例えばリストのバージョンナンバーが「０」か否かにより、相手方の光ディスク記録再生装置のデバイスタイプを判定する。このステップＳ１３の判定において、例えばリストのバージョンナンバーが「０」となっており、前記デバイスタイプＤｅｖ１（光ディスク記録再生装置３００）であると判定した場合、セキュリティモジュール１３の処理は、ステップＳ１４に進む。一方、ステップＳ１３の判定において、リストのバージョンナンバーが「０」でなく、前記デバイスタイプＤｅｖ２（光ディスク記録再生装置１００）であると判定した場合、セキュリティモジュール１３の処理は、ステップＳ１５に進む。

【０６２９】

ステップＳ１４の処理に進むと、セキュリティモジュール１３は、不揮発性メモリ３４に格納しているリストを用いて光ディスク記録再生装置３００のID_Bを検証し、その検証をパスしたとき、上記リストを光ディスク記録再生装置３００に送信した後、ステップＳ１９の処理に進む。

【０６３０】

また、ステップＳ１５の処理に進むと、セキュリティモジュール１３は、不揮発性メモリ３４に格納しているリストのバージョンが、光ディスク記録再生装置１００が保持するリストのバージョンナンバーよりも大きい（Ａ＞Ｂ）か、或いは等しいか（Ａ＝Ｂ）、或いは小さいか（Ａ＜Ｂ）の判定を行う。このステップＳ１５の判定において、Ａ＞Ｂであると判定した場合、セキュリティモジュール１３の処理はステップＳ１６に進み、Ａ＝Ｂであると判定した場合、セキュリティモジュール１３の処理はステップＳ１７に進み、Ａ＞Ｂであると判定した場合、セキュリティモジュール１３の処理はステップＳ１８に進む。

【０６３１】

ステップＳ１６の処理に進むと、セキュリティモジュール１３は、自己が保持するリストを用いて光ディスク記録再生装置１００のID_Bの検証を行い、そのリストを光ディスク記録再生装置１００に送信した後、ステップＳ１９に進む。

【０６３２】

また、ステップＳ１７の処理に進むと、セキュリティモジュール１３は、自己が保持するリストを用いて光ディスク記録再生装置１００のID_Bの検証を行った後、ステップＳ１９に進む。

【０６３３】

また、ステップＳ１８の処理に進むと、セキュリティモジュール１３は、光ディスク記録再生装置１００からリストを受信し、そのバージョンナンバー（RevV_B，RegV_B）の検証と、当該リストを用いた光ディスク記録再生装置１００のID_Bの検証と、センタＴＣの署名ＴＣSigの検証を行った後、ステップＳ１９に進む。

【０６３４】

ステップＳ１９の処理に進むと、セキュリティモジュール１３は、光ディスク記録再生装置から記録又は再生の何れの処理が要求されているのか判定する。

【０６３５】

当該ステップＳ１９にて記録の処理が要求されていると判定した場合、セキュリティモジュール１３は、ステップＳ２０の処理として、光ディスク記録再生装

置がセッション鍵Ｋseにて暗号鍵Ｋcoを暗号化した値Ｅnc（Kse，Kco）を受信して復号し、次に、その復号により得られた暗号鍵Ｋcoを自己が保持するストレージ鍵Ｋstで暗号化した値Ｅnc（Kst，Kco）を生成して光ディスク記録再生装置に送信する。その後、光ディスク記録再生装置において上記暗号鍵Ｋcoにて暗号化されたコンテンツデータＥnc（Kse，Kco）が、光ディスク１２に記録されることになる。

【０６３６】

一方、ステップＳ１９にて再生の処理が要求されていると判定した場合、セキュリティモジュール１３は、ステップＳ２１の処理として、ストレージ鍵Ｋstにて暗号鍵Ｋcoが暗号化され例えば光ディスク１２のデータ記録領域等に記録されている値Ｅnc（Kst，Kco）を読み出して復号し、その復号により得られた暗号鍵Ｋcoをセッション鍵Ｋseにて暗号化した値Ｅnc（Kse，Kco）を生成して光ディスク記録再生装置に送信する。その後、上記暗号鍵Ｋcoにて暗号化されているコンテンツデータＥnc（Kse，Kco）は、光ディスク１２から再生されて光ディスク記録再生装置に送られることになる。

【０６３７】

図８３には、前記メディアタイプＩＭ３に相当するメモリ情報記録媒体６０のセキュリティモジュール６３における処理の流れを示す。

【０６３８】

この図８３において、セキュリティモジュール６３は、ステップＳ３１として、前述したように、メモリ記録再生装置が発生した乱数R_Bの受信と、前記$V_A = K_A \cdot G$の計算、乱数R_Aの発生、デジタル署名を行いSig_A計算、$Cert_A$，R_A，R_B，V_A，$RevV_A$，$RegV_A$，Sig_Aをメモリ記録再生装置に送信する。

【０６３９】

次に、セキュリティモジュール６３は、ステップＳ３２として、メモリ記録再生装置から送信されてきた$Cert_B$，R_B，R_A，V_B，$RevV_B$，$RegV_B$，Sig_B受信、$Cert_B$の検証、Sig_Bの検証、セッション鍵Ｋseの計算を行う。

【０６４０】

次に、セキュリティモジュール６３は、ステップＳ３３として、例えばリスト

のバージョンナンバーが「０」か否かにより、相手方のメモリ記録再生装置のデバイスタイプを判定する。このステップＳ３３の判定において、例えばリストのバージョンナンバーが「０」となっており、前記デバイスタイプＤｅｖ３（メモリ記録再生装置４００）であると判定した場合、セキュリティモジュール６３の処理は、ステップＳ３４に進む。一方、ステップＳ３３の判定において、リストのバージョンナンバーが「０」でなく、前記デバイスタイプＤｅｖ４（メモリ記録再生装置２００）であると判定した場合、セキュリティモジュール６３の処理は、ステップＳ３５に進む。

【０６４１】

ステップＳ３４の処理に進むと、セキュリティモジュール６３は、メモリ部２２のデータ記録領域に格納しているリストを用いてメモリ記録再生装置４００のID_Bを検証し、その検証をパスしたとき、上記リストをメモリ記録再生装置４００に送信した後、ステップＳ３９の処理に進む。

【０６４２】

また、ステップＳ３５の処理に進むと、セキュリティモジュール６３は、メモリ部２２のデータ記録領域に格納しているリストのバージョンが、メモリ記録再生装置２００が保持するリストのバージョンナンバーよりも大きい（Ａ＞Ｂ）か、或いは等しいか（Ａ＝Ｂ）、或いは小さいか（Ａ＜Ｂ）の判定を行う。このステップＳ３５の判定において、Ａ＞Ｂであると判定した場合、セキュリティモジュール６３の処理はステップＳ３６に進み、Ａ＝Ｂであると判定した場合、セキュリティモジュール６３の処理はステップＳ３７に進み、Ａ＞Ｂであると判定した場合、セキュリティモジュール６３の処理はステップＳ３８に進む。

【０６４３】

ステップＳ３６の処理に進むと、セキュリティモジュール６３は、メモリ部２２のデータ記録領域に記録されていたリストを読み出し、そのバージョンナンバー（$RevV_A$, $RegV_A$）の検証と、当該リストを用いたメモリ記録再生装置２００のID_Bの検証と、センタＴＣの署名ＴＣSigの検証を行い、さらに当該リストをメモリ記録再生装置２００に送信した後、ステップＳ３９に進む。

【０６４４】

また、ステップＳ３７の処理に進むと、セキュリティモジュール６３は、メモリ部２２のデータ記録領域に記録されていたリストを読み出し、そのバージョンナンバー（$RevV_A$，$RegV_A$）の検証と、当該リストを用いたメモリ記録再生装置２００のID_Bの検証と、センタＴＣの署名ＴＣSigの検証を行った後、ステップＳ３９に進む。

【０６４５】

また、ステップＳ３８の処理に進むと、セキュリティモジュール６３は、メモリ記録再生装置２００からリストを受信し、そのバージョンナンバー（$RevV_B$，$RegV_B$）の検証と、当該リストを用いたメモリ記録再生装置２００のID_Bの検証と、センタＴＣの署名ＴＣSigの検証を行い、さらに、そのリストをメモリ部２２に書き込んで更新した後、ステップＳ３９に進む。

【０６４６】

ステップＳ３９の処理に進むと、セキュリティモジュール６３は、メモリ記録再生装置から記録又は再生の何れの処理が要求されているのか判定する。

【０６４７】

当該ステップＳ３９にて記録の処理が要求されていると判定した場合、セキュリティモジュール６３は、ステップＳ４０の処理として、メモリ記録再生装置がセッション鍵Ｋseにて暗号鍵Ｋcoを暗号化した値Ｅnc（Kse，Kco）を受信して復号し、次に、その復号により得られた暗号鍵Ｋcoを自己が保持するストレージ鍵Ｋstで暗号化した値Ｅnc（Kst，Kco）を生成してメモリ記録再生装置に送信する。その後、セキュリティモジュール６３は、上記メモリ記録再生装置において上記暗号鍵Ｋcoにて暗号化されたコンテンツデータＥnc（Kse，Kco）を受信し、メモリ部２２に記録する。

【０６４８】

一方、ステップＳ３９にて再生の処理が要求されていると判定した場合、セキュリティモジュール６３は、ステップＳ４１の処理として、ストレージ鍵Ｋstにて暗号鍵Ｋcoが暗号化され例えばメモリ部２２のデータ記録領域等に記録されている値Ｅnc（Kst，Kco）を読み出して復号し、その復号により得られた暗号鍵Ｋ

coをセッション鍵Ｋseにて暗号化した値Ｅnc（Kse, Kco）を生成してメモリ記録再生装置に送信する。その後、セキュリティモジュール６３は、メモリ部２２から上記暗号鍵Ｋcoにて暗号化されているコンテンツデータＥnc（Kse, Kco）を読み出し、メモリ記録再生装置に送る。

【０６４９】

図８４には、前記メディアタイプＩＭ４に相当するメモリ情報記録媒体２０のセキュリティモジュール２３における処理の流れを示す。

【０６５０】

この図８４において、セキュリティモジュール２３は、ステップＳ５１として、前述したように、メモリ記録再生装置が発生した乱数R_Bの受信と、前記V_A＝~~K_A・Gの計算、乱数R_Aの発生、デジタル署名を行いSig_A計算、$Cert_A$、R_A、~~R_B、V_A、$RevV_A$、$RegV_A$、Sig_Aをメモリ記録再生装置に送信する。

【０６５１】

次に、セキュリティモジュール２３は、ステップＳ５２として、メモリ記録再生装置から送信されてきた$Cert_B$、R_B、R_A、V_B、$RevV_B$、$RegV_B$、Sig_B受信、$Cert_B$の検証、Sig_Bの検証、セッション鍵Ｋseの計算を行う。

【０６５２】

次に、セキュリティモジュール２３は、ステップＳ５３として、例えばリストのバージョンナンバーが「０」か否かにより、相手方のメモリ記録再生装置のデバイスタイプを判定する。このステップＳ５３の判定において、例えばリストのバージョンナンバーが「０」となっており、前記デバイスタイプＤｅｖ３（メモリ記録再生装置４００）であると判定した場合、セキュリティモジュール２３の処理は、ステップＳ５４に進む。一方、ステップＳ５３の判定において、リストのバージョンナンバーが「０」でなく、前記デバイスタイプＤｅｖ４（メモリ記録再生装置２００）であると判定した場合、セキュリティモジュール２３の処理は、ステップＳ５５に進む。

【０６５３】

ステップＳ５４の処理に進むと、セキュリティモジュール２３は、不揮発性メモリ４４に格納しているリストを用いてメモリ記録再生装置４００のID_Bを検

証し、その検証をパスしたとき、上記リストをメモリ記録再生装置４００に送信した後、ステップＳ５９の処理に進む。

【０６５４】

また、ステップＳ５５の処理に進むと、セキュリティモジュール２３は、不揮発性メモリ４４に格納しているリストのバージョンが、メモリ記録再生装置２００が保持するリストのバージョンナンバーよりも大きい（Ａ＞Ｂ）か、或いは等しいか（Ａ＝Ｂ）、或いは小さいか（Ａ＜Ｂ）の判定を行う。このステップＳ５５の判定において、Ａ＞Ｂであると判定した場合、セキュリティモジュール２３の処理はステップＳ５６に進み、Ａ＝Ｂであると判定した場合、セキュリティモジュール２３の処理はステップＳ５７に進み、Ａ＞Ｂであると判定した場合、セキュリティモジュール２３の処理はステップＳ５８に進む。

【０６５５】

ステップＳ５６の処理に進むと、セキュリティモジュール２３は、自己が保持するリストを用いてメモリ記録再生装置２００のＩＤ$_B$の検証を行い、そのリストをメモリ記録再生装置１００に送信した後、ステップＳ５９に進む。

【０６５６】

また、ステップＳ５７の処理に進むと、セキュリティモジュール２３は、自己が保持するリストを用いてメモリ記録再生装置２００のＩＤ$_B$の検証を行った後、ステップＳ５９に進む。

【０６５７】

また、ステップＳ５８の処理に進むと、セキュリティモジュール２３は、メモリ記録再生装置２００からリストを受信し、そのバージョンナンバー（ＲｅｖV_B，ＲｅｇV_B）の検証と、当該リストを用いたメモリ記録再生装置２００のＩＤ$_B$の検証と、センタＴＣの署名ＴＣＳｉｇの検証を行った後、ステップＳ５９に進む。

【０６５８】

ステップＳ５９の処理に進むと、セキュリティモジュール２３は、メモリ記録再生装置から記録又は再生の何れの処理が要求されているのか判定する。

【０６５９】

当該ステップＳ５９にて記録の処理が要求されていると判定した場合、セキュ

リティモジュール２３は、ステップＳ６０の処理として、メモリ記録再生装置がセッション鍵Ｋseにて暗号鍵Ｋcoを暗号化した値Ｅnc（Kse，Kco）を受信して復号し、次に、その復号により得られた暗号鍵Ｋcoを自己が保持するストレージ鍵Ｋstで暗号化した値Ｅnc（Kst，Kco）を生成して光ディスク記録再生装置に送信する。その後、セキュリティモジュール２３は、上記メモリ記録再生装置において上記暗号鍵Ｋcoにて暗号化されたコンテンツデータＥnc（Kse，Kco）を受信し、メモリ部２２に記録する。

【０６６０】

一方、ステップＳ５９にて再生の処理が要求されていると判定した場合、セキュリティモジュール２３は、ステップＳ６１の処理として、ストレージ鍵Ｋstにて暗号鍵Ｋcoが暗号化され例えばメモリ部２２のデータ記録領域等に記録されている値Ｅnc（Kst，Kco）を読み出して復号し、その復号により得られた暗号鍵Ｋcoをセッション鍵Ｋseにて暗号化した値Ｅnc（Kse，Kco）を生成してメモリ記録再生装置に送信する。その後、上記暗号鍵Ｋcoにて暗号化されているコンテンツデータＥnc（Kse，Kco）は、メモリ部２２から再生されてメモリ記録再生装置に送られることになる。

【０６６１】

次に、前記デバイスタイプＤｅｖ１～Ｄｅｖ４に相当する各光ディスク記録再生装置、メモリ記録再生装置における処理の流れを示す。なお、デバイスタイプＤｅｖ１に相当する光ディスク記録再生装置３００とデバイスタイプＤｅｖ３に相当するメモリ記録再生装置４００の処理の流れは略々同じであり、また、デバイスタイプＤｅｖ２に相当する光ディスク記録再生装置１００とデバイスタイプＤｅｖ４に相当するメモリ記録再生装置２００の処理の流れは略々同じであるため、以下の説明では、デバイスタイプＤｅｖ１及びＤｅｖ３での処理と、デバイスタイプＤｅｖ２及びＤｅｖ４での処理を、それぞれ纏めて説明する。

【０６６２】

図８５には、デバイスタイプＤｅｖ１及びＤｅｖ３の記録再生装置の処理の流れを示す。

【０６６３】

この図８５において、記録再生装置は、ステップＳ７１の処理として、先ず、乱数R_Bを発生して情報記録媒体に送信する。

【０６６４】

次に、記録再生装置は、ステップＳ７２の処理として、情報記録媒体から送信されてきた$Cert_A$，R_A，R_B，V_A，$RevV_A$，$RegV_A$，Sig_Aを受信する。またお、メディア記録再生装置に送信し、$Cert_A$の検証、Sig_Aの検証、前記$V_B=K_B \cdot G$の計算を行った後、情報記録媒体に対して、$Cert_B$，R_B，R_A，V_B，$RevV_B$，$RegV_B$，Sig_Bを送信する。なお、このときバージョンナンバー$RevV_B$，$RegV_B$は「０」となる。

【０６６５】

次に、記録再生装置は、ステップＳ７３の処理として、セッション鍵Ｋseの計算を行う。

【０６６６】

次に、記録再生装置は、ステップＳ７４として、情報記録媒体のメディアタイプが、ＩＭ１か或いはそれ以外（ＩＭ２，ＩＭ３，ＩＭ４）か否かの判定を行う。当該ステップＳ７４の判定において、情報記録媒体がメディアタイプＩＭ１であると判定した場合、記録再生装置の処理はステップＳ７５に進み、情報記録媒体がメディアタイプＩＭ１でない（メディアタイプＩＭ２，ＩＭ３，ＩＭ４）であると判定した場合、記録再生装置の処理はステップＳ７６に進む。

【０６６７】

ステップＳ７５の処理に進むと、記録再生装置は、メディアタイプＩＭ１の光ディスク情報記録媒体５０の光ディスク１２からリボケーションリスト／レジストレーションリストを読み出し、そのリストのバージョンナンバー（$RevV_A$，$RegV_A$）の検証と、そのリストを用いた光ディスク情報記録媒体５０のID_Aの検証と、センタＴＣの署名ＴＣSigの検証を行い、そのリストを光ディスク情報記録媒体５０のセキュリティモジュール５３に送信した後、ステップＳ７７に進む。

【０６６８】

また、ステップＳ７６の処理に進むと、記録再生装置は、メディアタイプＩＭ１でないメディアタイプ（ＩＭ２～ＩＭ４）の情報記録媒体からリボケーションリスト／レジストレーションリストを読み出し、そのリストのバージョンナンバー（$RevV_A$, $RegV_A$）の検証と、そのリストを用いた情報記録媒体のID_Aの検証と、センタＴＣの署名ＴＣSigの検証を行った後、ステップＳ７７に進む。

【０６６９】

ステップＳ７７の処理に進むと、記録再生装置は、情報記録媒体に対してデータの記録を行うのか、或いは情報記録媒体からデータの再生を行うのか判定する。

【０６７０】

当該ステップＳ７７にて記録の処理を行うと判定した場合、記録再生装置は、ステップＳ７８の処理として、再度、メディアタイプが、ＩＭ１，ＩＭ２（すなわち光ディスク情報記録媒体）であるか、或いはＩＭ３，ＩＭ４（すなわちメモリ情報記録媒体）であるかの判定を行う。当該ステップＳ７８の判定において、情報記録媒体がメディアタイプＩＭ１，ＩＭ２であると判定した場合、記録再生装置の処理はステップＳ８０に進み、情報記録媒体がメディアタイプＩＭ３，ＩＭ４であると判定した場合、記録再生装置の処理はステップＳ８１に進む。

【０６７１】

また、上記ステップＳ７７にて再生の処理を行うと判定した場合、記録再生装置は、ステップＳ７９の処理として、再度、メディアタイプが、ＩＭ１，ＩＭ２（光ディスク情報記録媒体）であるか、或いはＩＭ３，ＩＭ４（メモリ情報記録媒体）であるかの判定を行う。当該ステップＳ７９の判定において、情報記録媒体がメディアタイプＩＭ１，ＩＭ２であると判定した場合、記録再生装置の処理はステップＳ８２に進み、情報記録媒体がメディアタイプＩＭ３，ＩＭ４であると判定した場合、記録再生装置の処理はステップＳ８３に進む。

【０６７２】

上記ステップＳ８０の処理に進むと、記録再生装置は、セッション鍵Ｋseにて暗号鍵Ｋcoを暗号化した値Ｅnc（Kse, Kco）を送信し、それに対応して情報記録

媒体がストレージ鍵Ｋstで暗号鍵Ｋcoを暗号化して送信してきた値Ｅnc（Kst，Kco）を受信した後、ストレージ鍵Ｋstで暗号鍵Ｋcoを暗号化した値Ｅnc（Kst，Kco）と暗号鍵Ｋcoでコンテンツデータを暗号化したデータＥnc（Kco，data）を情報記録媒体に書き込む。

【０６７３】

また、ステップＳ８１の処理に進むと、記録再生装置は、セッション鍵Ｋseにて暗号鍵Ｋcoを暗号化した値Ｅnc（Kse，Kco）を送信した後、暗号鍵Ｋcoでコンテンツデータを暗号化したデータＥnc（Kco，data）を情報記録媒体に書き込む。

【０６７４】

また、ステップＳ８２の処理に進むと、記録再生装置は、ストレージ鍵Ｋstにて暗号鍵Ｋcoが暗号化された値Ｅnc（Kst，Kco）を情報記録媒体から読み出し、その値Ｅnc（Kst，Kco）を情報記録媒体のセキュリティモジュールに送信し、情報記録媒体が値Ｅnc（Kst，Kco）をストレージ鍵Ｋstで復号し、さらにその暗号鍵Ｋcoをセッション鍵Ｋseで暗号化した値Ｅnc（Kse，Kco）を受信した後、当該暗号鍵Ｋcoで暗号化されているコンテンツデータＥnc（Kco，data）を情報記録媒体から読み出す。

【０６７５】

また、ステップＳ８３の処理に進むと、記録再生装置は、セッション鍵Ｋseにて暗号鍵Ｋcoを暗号化した値Ｅnc（Kse，Kco）を情報記録媒体から受信した後、当該暗号鍵Ｋcoで暗号化されているコンテンツデータＥnc（Kco，data）を情報記録媒体から読み出す。

【０６７６】

図８６及び図８７には、デバイスタイプＤｅｖ２及びＤｅｖ３の記録再生装置の処理の流れを示す。なお、図８６と図８７は、本来は１つの図面上に描く冪であるが、紙面の都合で２つの図に分けている。

【０６７７】

この図８６において、記録再生装置は、ステップＳ９１の処理として、先ず、乱数R_Bを発生して情報記録媒体に送信する。

【０６７８】

次に、記録再生装置は、ステップＳ９２の処理として、情報記録媒体から送信されてきた$Cert_A$，R_A，R_B，V_A，$RevV_A$，$RegV_A$，Sig_Aを受信する。またお、メディア記録再生装置に送信し、$Cert_A$の検証、Sig_Aの検証、前記$V_B=K_B \cdot G$の計算を行った後、情報記録媒体に対して、$Cert_B$，R_B，R_A，V_B，$RevV_B$，$RegV_B$，Sig_Bを送信する。

【０６７９】

次に、記録再生装置は、ステップＳ９３の処理として、セッション鍵Ｋseの計算を行う。

【０６８０】

次に、記録再生装置は、ステップＳ９４として、情報記録媒体のメディアタイプが、ＩＭ１か或いはそれ以外（ＩＭ２，ＩＭ３，ＩＭ４）か否かの判定を行う。当該ステップＳ９４の判定において、情報記録媒体がメディアタイプＩＭ１であると判定した場合、記録再生装置の処理はステップＳ９５に進み、情報記録媒体がメディアタイプＩＭ１でない（メディアタイプＩＭ２，ＩＭ３，ＩＭ４）であると判定した場合、記録再生装置の処理はステップＳ９６に進む。

【０６８１】

ステップＳ９５の処理に進むと、記録再生装置は、上記$RevV_A$，$RegV_A$と、$RevV_B$，$RegV_B$からバージョンの新しさの判断を行う。すなわち記録再生装置は、そのリストのバージョンが、記録再生装置の保持するバージョンナンバーよりも大きい（Ａ＞Ｂ）か、或いは等しいか（Ａ＝Ｂ）、或いは小さいか（Ａ＜Ｂ）の判定を行う。このステップＳ９５の判定において、Ａ＞Ｂであると判定した場合、記録再生装置の処理はステップＳ９７に進み、Ａ＝Ｂであると判定した場合、記録再生装置の処理はステップＳ９８に進み、Ａ＞Ｂであると判定した場合、記録再生装置の処理はステップＳ９９に進む。

【０６８２】

ステップＳ９７の処理に進むと、記録再生装置は、メディアタイプＩＭ１の光ディスク情報記録媒体５０の光ディスク１２からリボケーションリスト／レジストレーションリストを読み出し、そのリストのバージョンナンバー（$RevV_A$，

$RegV_A$）の検証と、そのリストを用いた光ディスク情報記録媒体５０のID_Aの検証と、センタＴＣの署名ＴＣSigの検証を行い、そのリストを光ディスク情報記録媒体５０のセキュリティモジュール５３に送信した後、図８７のステップＳ１１０の処理に進む。

【０６８３】

また、ステップＳ９８の処理に進むと、記録再生装置は、自己が保持するリストを用いて情報記録媒体ID_Aの検証を行い、当該リストを情報記録媒体の送信した後、図８７のステップＳ１１０の処理に進む。

【０６８４】

また、ステップＳ９９の処理に進むと、記録再生装置は、自己が保持するリストを用いて情報記録媒体ID_Aの検証を行い、当該リストを情報記録媒体の送信する。さらに、記録再生装置は、ステップＳ１０３で、上記情報記録媒体に対して当該リストを書き込ませ（更新）た後、図８７のステップＳ１１０の処理に進む。

【０６８５】

一方、上記ステップＳ９６の処理に進むと、記録再生装置は、上記$RevV_A$, $RegV_A$と、$RevV_B$, $RegV_B$からバージョンの新しさの判断を行う。すなわち記録再生装置は、そのリストのバージョンが、記録再生装置の保持するバージョンナンバーよりも大きい（Ａ＞Ｂ）か、或いは等しいか（Ａ＝Ｂ）、或いは小さいか（Ａ＜Ｂ）の判定を行う。このステップＳ９６の判定において、Ａ＞Ｂであると判定した場合、記録再生装置の処理はステップＳ１００に進み、Ａ＝Ｂであると判定した場合、記録再生装置の処理はステップＳ１０１に進み、Ａ＞Ｂであると判定した場合、記録再生装置の処理はステップＳ１０２に進む。

【０６８６】

ステップＳ１００の処理に進むと、記録再生装置は、メディアタイプＩＭ２～ＩＭ４の情報記録媒体からリボケーションリスト／レジストレーションリストを読み出し、そのリストのバージョンナンバー（$RevV_A$, $RegV_A$）の検証と、そのリストを用いた情報記録媒体のID_Aの検証と、センタＴＣの署名ＴＣSigの検証を行い、その後、図８７のステップＳ１１０の処理に進む。

【０６８７】

また、ステップＳ１０１の処理に進むと、記録再生装置は、自己が保持するリストを用いて情報記録媒体$ＩＤ_{A}$の検証を行った後、図８７のステップＳ１１０の処理に進む。

【０６８８】

また、ステップＳ１０２の処理に進むと、記録再生装置は、自己が保持するリストを用いて情報記録媒体$ＩＤ_{A}$の検証を行い、当該リストを情報記録媒体に送信した後、図８７のステップＳ１１０の処理に進む。

【０６８９】

図８７のステップＳ１１０の処理に進むと、記録再生装置は、情報記録媒体に対してデータの記録を行うのか、或いは情報記録媒体からデータの再生を行うのか判定する。

【０６９０】

当該ステップＳ１１０にて記録の処理を行うと判定した場合、記録再生装置は、ステップＳ１１１の処理として、再度、メディアタイプが、ＩＭ１，ＩＭ２（光ディスク情報記録媒体）であるか、或いはＩＭ３，ＩＭ４（メモリ情報記録媒体）であるかの判定を行う。当該ステップＳ１１１の判定において、情報記録媒体がメディアタイプＩＭ１，ＩＭ２であると判定した場合、記録再生装置の処理はステップＳ１１３に進み、情報記録媒体がメディアタイプＩＭ３，ＩＭ４であると判定した場合、記録再生装置の処理はステップＳ１１４に進む。

【０６９１】

また、上記ステップＳ１１０にて再生の処理を行うと判定した場合、記録再生装置は、ステップＳ１１２の処理として、再度、メディアタイプが、ＩＭ１，ＩＭ２（光ディスク情報記録媒体）であるか、或いはＩＭ３，ＩＭ４（メモリ情報記録媒体）であるかの判定を行う。当該ステップＳ１１２の判定において、情報記録媒体がメディアタイプＩＭ１，ＩＭ２であると判定した場合、記録再生装置の処理はステップＳ１１５に進み、情報記録媒体がメディアタイプＩＭ３，ＩＭ４であると判定した場合、記録再生装置の処理はステップＳ１１６に進む。

【０６９２】

上記ステップＳ１１３の処理に進むと、記録再生装置は、セッション鍵Ｋseにて暗号鍵Ｋcoを暗号化した値Ｅnc（Kse，Kco）を送信し、それに対応して情報記録媒体がストレージ鍵Ｋstで暗号鍵Ｋcoを暗号化して送信してきた値Ｅnc（Kst，Kco）を受信した後、ストレージ鍵Ｋstで暗号鍵Ｋcoを暗号化した値Ｅnc（Kst，Kco）と暗号鍵Ｋcoでコンテンツデータを暗号化したデータＥnc（Kco，data）を情報記録媒体に書き込む。

【０６９３】

また、ステップＳ１１４の処理に進むと、記録再生装置は、セッション鍵Ｋseにて暗号鍵Ｋcoを暗号化した値Ｅnc（Kse，Kco）を送信した後、暗号鍵Ｋcoでコンテンツデータを暗号化したデータＥnc（Kco，data）を情報記録媒体に書き込む。

【０６９４】

また、ステップＳ１１５の処理に進むと、記録再生装置は、ストレージ鍵Ｋstにて暗号鍵Ｋcoが暗号化された値Ｅnc（Kst，Kco）を情報記録媒体から読み出し、その値Ｅnc（Kst，Kco）を情報記録媒体のセキュリティモジュールに送信し、情報記録媒体が値Ｅnc（Kst，Kco）をストレージ鍵Ｋstで復号し、さらにその暗号鍵Ｋcoをセッション鍵Ｋseで暗号化した値Ｅnc（Kse，Kco）を受信した後、当該暗号鍵Ｋcoで暗号化されているコンテンツデータＥnc（Kco，data）を情報記録媒体から読み出す。

【０６９５】

また、ステップＳ１１６の処理に進むと、記録再生装置は、セッション鍵Ｋseにて暗号鍵Ｋcoを暗号化した値Ｅnc（Kse，Kco）を情報記録媒体から受信した後、当該暗号鍵Ｋcoで暗号化されているコンテンツデータＥnc（Kco，data）を情報記録媒体から読み出す。

【０６９６】

なお、上述した実施の形態では、本発明を適用した情報記録媒体として光ディスク記録媒体とメモリ情報記録媒体の例を提示したが、情報記録媒体はこれに限るものではなく、磁気ディスクや磁気テープ、光磁気ディスク、バッテリーバッ

クアップされた揮発性メモリなどでもよい。

【０６９７】

次に、上述した本発明の情報記録媒体を製造する本発明の記録媒体製造装置及び方法について説明する。

【０６９８】

以下に、本発明の情報記録媒体として前述した実施の形態のメディアタイプＩＭ１～ＩＭ４の各情報記録媒体を例に挙げ、それら各メディアタイプＩＭ１～ＩＭ４の情報記録媒体をそれぞれ製造する記録媒体製造装置について説明を行う。

【０６９９】

図８８には、メディアタイプＩＭ１の光ディスク情報記録媒体５０を製造すると共に、当該光ディスク情報記録媒体５０に対して最新のリストを記録する記録媒体製造装置である光ディスク製造装置５００の概略構成を示す。なお、記録する最新のリストは、リボケーションリスト又はレジストレーションリストの一方、或いは、リボケーションリスト及びレジストレーションリストの両方の何れであっても良い。

【０７００】

この図８８に示す光ディスク製造装置５００は、図示しない組立工程により既に組み立てられている光ディスク情報記録媒体５０に対して、リストを記録する。但し、メディアタイプＩＭ１である光ディスク情報記録媒体５０は、前述したようにセキュリティモジュール５３がリストを格納するための不揮発性メモリを備えていないか、或いは不揮発性メモリがリストを格納するのに十分な記憶容量を備えていないため、当該光ディスク製造装置５００は、光ディスク情報記録媒体５０のコンテンツデータ記録用の領域に上記リストを記録する。

【０７０１】

このため、当該光ディスク製造装置５００は、光ディスク情報記録媒体５０のカートリッジ１１内の光ディスク１２を回転させるスピンドルモータ５０１と、光ディスク１２のデータ記録領域に情報を少なくとも書き込み可能な光学ヘッド５０２と、スピンドルモータ５０１や光学ヘッド５０２のサーボ回路５０３と、これらを制御する制御部５０５等を備えている。

【０７０２】

さらに、光ディスク製造装置５００は、光ディスク情報記録媒体５０のＩＤ、秘密鍵、公開鍵証明書、当該媒体５０の製造時点における最新のリスト及びそのバージョンナンバーを予め格納している鍵・リスト記録媒体５０７と、そのドライブ部６０６と、光ディスク情報記録媒体５０のセキュリティモジュール５３との間で情報の授受を行うインターフェース部５０８とを備えている。なお、図８８の構成では、鍵・リスト記録媒体５０７及びドライブ部５０６は、当該光ディスク製造装置５００に内蔵されている例を挙げているが、当該鍵・リスト記録媒体５０７及びドライブ部５０６は外付けの媒体及びドライブであってもよい。上記ＩＤ、秘密鍵、公開鍵証明書、最新のリスト及びバージョンナンバーは、例えば図示しない鍵発行センタにより発行されるものであサ、上記内蔵或いは外付けの鍵・リスト記録媒体に予め格納されている。

【０７０３】

上記鍵・リスト記録媒体５０７に格納されている情報は、制御部５０５の制御の元、ドライブ部５０６により読み取られ、当該読み取られた情報のうち、上記ＩＤ、秘密鍵、公開鍵証明書、バージョンナンバーについてはインターフェース部５０８から光ディスク情報記録媒体５０のセキュリティモジュール５３に送られて記憶され、上記最新のリストは光学ヘッド５０２にて光ディスク１２のデータ記録領域に記録される。

【０７０４】

また、ＩＤ、秘密鍵、公開鍵証明書、最新のリスト及びそのバージョンナンバーは、上述したように内蔵或いは外付けの鍵・リスト記録媒体に予め格納されているものを読み取るだけでなく、例えば鍵発行センタより送られてきたものを外部インターフェース部５０９を介して直接に入手することも可能である。このように、外部インターフェース部５０９を介してＩＤ、秘密鍵、公開鍵証明書、最新のリスト及びそのバージョンナンバーを入手するようにした場合、当該外部インターフェース部５０９を介したＩＤ、秘密鍵、公開鍵証明書、バージョンナンバーは制御部５０５からインターフェース部５０８に直接送られて光ディス情報記録媒体５０のセキュリティモジュール５３に記憶され、上記最新のリストは制

御部５０５から光学ヘッド５０２に直接送られて光ディスク１２のデータ記録領域に記録されることになる。

【０７０５】

図８９には、本発明の記録媒体製造方法として、上記メディアタイプＩＭ１の光ディスク情報記録媒体５０を製造すると共に、当該光ディスク情報記録媒体５０に対して最新のリストを記録する光ディスク製造方法における製造工程の流れを示す。

【０７０６】

図８９において、光ディスク製造方法では、先ず、ステップＳ２００の製造工程として、図示しない組立工程によりメディアタイプＩＭ１の光ディスク情報記録媒体５０が組み立てられる。

【０７０７】

次に、光ディスク製造方法では、ステップＳ２０１の製造工程として、図８８の光ディスク製造装置５００により、前記ＩＤ、秘密鍵、公開鍵証明書、バージョンナンバーを、メディアタイプＩＭ１である光ディスク情報記録媒体５０のセキュリティモジュール５３内に設けられている不揮発性の鍵メモリ３６に書き込む。

【０７０８】

次に、光ディスク製造方法では、ステップＳ２０２の製造工程として、図８８の光ディスク製造装置５００により、最新のリストを光ディスク１２のコンテンツデータ記録用の領域に書き込む。

【０７０９】

以上により、光ディスク情報記録媒体５０は、最新版のリストをデータ記録領域に記録した状態で製造工場から出荷されることになる。

【０７１０】

図９０には、メディアタイプＩＭ２の光ディスク情報記録媒体１０を製造すると共に、当該光ディスク情報記録媒体１０に対して最新のリストを記録する記録媒体製造装置である光ディスク製造装置５１０の概略構成を示す。なお、記録する最新のリストは、リボケーションリスト又はレジストレーションリストの一方

、或いは、リボケーションリスト及びレジストレーションリストの両方の何れであっても良い。

【０７１１】

この図９０に示す光ディスク製造装置５１０は、図示しない組立工程により既に組み立てられている光ディスク情報記録媒体１０に対して、リストを記録する。但し、メディアタイプＩＭ２である光ディスク情報記録媒体１０は、前述したようにセキュリティモジュール１３がリストを格納するための充分な記憶容量を有する不揮発性メモリ（３４）を備えているため、当該光ディスク製造装置５１０は、光ディスク情報記録媒体１０のセキュリティモジュール１３の不揮発性メモリに上記リストを記録する。

【０７１２】

このため、当該光ディスク製造装置５１０は、少なくとも、光ディスク情報記録媒体１０のセキュリティモジュール１３にリストを送信するためのインターフェース部５１８と、各部を制御する制御部５１５等を備えている。なお、図９０の例では、図５８の例のようにスピンドルモータや光学ヘッド等を備えていない構成を挙げているが、光ディスク製造装置５１０はもちろんそれらを備えていてもよい。

【０７１３】

さらに、光ディスク製造装置５１０は、光ディスク情報記録媒体１０のＩＤ、秘密鍵、公開鍵証明書、当該媒体１０の製造時点における最新のリスト及びそのバージョンナンバーを予め格納している鍵・リスト記録媒体５１７とそのドライブ部５１６も備えている。なお、図９０の構成では、鍵・リスト記録媒体５１７及びドライブ部５１６は、当該光ディスク製造装置５１０に内蔵されている例を挙げているが、当該鍵・リスト記録媒体５１７及びドライブ部５１６は外付けの媒体及びドライブであってもよい。上記ＩＤ、秘密鍵、公開鍵証明書、最新のリスト及びバージョンナンバーは、図示しない鍵発行センタにより発行されるものであり、上記内蔵或いは外付けの鍵・リスト記録媒体に予め格納されている。

【０７１４】

上記鍵・リスト記録媒体５１７に格納されている情報は、制御部５１５の制御

の元、ドライブ部５１６により読み取られ、インターフェース部５１８から光ディスク情報記録媒体１０のセキュリティモジュール１３に送られて不揮発性メモリ（３４）に記憶される。

【０７１５】

また、この図９０の例でも前記図８８の場合と同様に、ＩＤ、秘密鍵、公開鍵証明書、最新のリスト及びそのバージョンナンバーは、上述した内蔵或いは外付けの鍵・リスト記録媒体に予め格納されているものを読み取るだけでなく、鍵発行センタより送られてきたものを外部インターフェース部５１９を介して直接に入手することも可能である。外部インターフェース部５１９を介してＩＤ、秘密鍵、公開鍵証明書、最新のリスト及びそのバージョンナンバーを入手するようにした場合、当該外部インターフェース部５１９を介したＩＤ、秘密鍵、公開鍵証明書、最新のリスト及びそのバージョンナンバーは、制御部５１５からインターフェース部５１８に直接送られて光ディス情報記録媒体１０のセキュリティモジュール１３に送られて不揮発性メモリ３４に記録されることになる。

【０７１６】

図９１には、本発明の記録媒体製造方法として、上記メディアタイプＩＭ２の光ディスク情報記録媒体１０を製造すると共に、当該光ディスク情報記録媒体１０に対して最新のリストを記録する光ディスク製造方法における製造工程の流れを示す。

【０７１７】

図９１において、光ディスク製造方法では、先ず、ステップＳ２１０の製造工程として、図示しない組立工程によりメディアタイプＩＭ２の光ディスク情報記録媒体１０が組み立てられる。

【０７１８】

次に、光ディスク製造方法では、ステップＳ２１１の製造工程として、図９０の光ディスク製造装置５１０により、前記ＩＤ、秘密鍵、公開鍵証明書、バージョンナンバーを、メディアタイプＩＭ２である光ディスク情報記録媒体１０のセキュリティモジュール１３内に設けられている不揮発性メモリ３４に書き込む。

【０７１９】

次に、光ディスク製造方法では、ステップＳ２１２の製造工程として、図９０の光ディスク製造装置５１０により、最新のリストを光ディスク情報記録媒体１０のセキュリティモジュール１３内に設けられている不揮発性メモリ３４に書き込む。

【０７２０】

以上により、光ディスク記録再生装置１０は、セキュリティモジュール１３に最新版のリストを記録した状態で製造工場から出荷されることになる。

【０７２１】

図９２には、メディアタイプＩＭ３のメモリ情報記録媒体６０を製造すると共に、当該メモリ情報記録媒体６０に対して最新のリストを記録する記録媒体製造装置であるメモリ製造装置６００の概略構成を示す。なお、記録する最新のリストは、リボケーションリスト又はレジストレーションリストの一方、或いは、リボケーションリスト及びレジストレーションリストの両方の何れであっても良い。

【０７２２】

この図９２に示すメモリ製造装置６００は、図示しない組立工程により既に組み立てられているメモリ情報記録媒体６０に対して、リストを記録する。但し、メディアタイプＩＭ３であるメモリ情報記録媒体６０は、前述したようにセキュリティモジュール６３がリストを格納するための不揮発性メモリを備えていないか、或いは不揮発性メモリがリストを格納するのに十分な記憶容量を備えていないため、当該メモリ製造装置６００は、メモリ情報記録媒体６０のメモリ部２２のコンテンツデータ記録用の領域に上記リストを記録する。

【０７２３】

このため、当該メモリ製造装置６００は、少なくとも、メモリ情報記録媒体６０に信号を送信するためのインターフェース部６０８と、メモリ情報記録媒体６０の入出力端子２４に接続するための入出力端子６０１と、各部を制御する制御部６０５等を備えている。

【０７２４】

さらに、メモリ製造装置６００は、メモリ情報記録媒体６０のＩＤ、秘密鍵、公開鍵証明書、当該媒体６０の製造時点における最新のリスト及びそのバージョンナンバーを予め格納している鍵・リスト記録媒体６０７とそのドライブ部６０６を備えている。なお、図９２の構成では、鍵・リスト記録媒体６０７及びドライブ部６０６は、当該メモリ製造装置６００に内蔵されている例を挙げているが、当該鍵・リスト記録媒体６０７及びドライブ部６０６は外付けの媒体及びドライブであってもよい。上記ＩＤ、秘密鍵、公開鍵証明書、最新のリスト及びバージョンナンバーは、図示しない鍵発行センタにより発行されるものであり、上記内蔵或いは外付けの鍵・リスト記録媒体に予め格納されている。

【０７２５】

上記鍵・リスト記録媒体６０７に格納されている情報は、制御部６０５の制御の元、ドライブ部６０６により読み取られ、インターフェース部６０８及び入出力端子６０１を介して、メモリ情報記録媒体６０に送られる。このときのメモリ情報記録媒体６０では、メモリ製造装置６００から送られてきた上記ＩＤ、秘密鍵、公開鍵証明書、最新のリスト及びそのバージョンナンバーを、メモリ部２２のデータ記録領域に記録する。

【０７２６】

また、ＩＤ、秘密鍵、公開鍵証明書、最新のリスト及びそのバージョンナンバーは、上述したように内蔵或いは外付けの鍵・リスト記録媒体に予め格納されているものを読み取るだけでなく、例えば鍵発行センタより送られてきたものを外部インターフェース部６０９を介して直接に入手することも可能である。このように、外部インターフェース部６０９を介してＩＤ、秘密鍵、公開鍵証明書、最新のリスト及びそのバージョンナンバーを入手するようにした場合、当該外部インターフェース部６０９を介したＩＤ、秘密鍵、公開鍵証明書、最新のリスト及びそのバージョンナンバーは、制御部６０５からインターフェース部６０８、入出力端子６０１を介して直接メモリ情報記録媒体６０に送られ、メモリ部２２のデータ記録領域に記録されることになる。

【０７２７】

図９３には、本発明の記録媒体製造方法として、上記メディアタイプＩＭ３のメモリ情報記録媒体６０を製造すると共に、当該メモリ情報記録媒体６０に対して最新のリストを記録するメモリ製造方法における製造工程の流れを示す。

【０７２８】

図９３において、メモリ製造方法では、先ず、ステップＳ３００の製造工程として、図示しない組立工程によりメディアタイプＩＭ３のメモリ情報記録媒体６０が組み立てられる。

【０７２９】

次に、メモリ製造方法では、ステップＳ３０１の製造工程として、図９２のメモリ製造装置６００により、前記ＩＤ、秘密鍵、公開鍵証明書、バージョンナンバーを、メディアタイプＩＭ３であるメモリ情報記録媒体６０のメモリ部２２のデータ記録領域に書き込む。

【０７３０】

次に、メモリ製造方法では、ステップＳ３０２の製造工程として、図９２のメモリ製造装置６００により、最新のリストをメモリ部２２のコンテンツデータ記録用の領域に書き込む。

【０７３１】

以上により、メモリ情報記録媒体６０は、最新版のリストをデータ記録領域に記録した状態で製造工場から出荷されることになる。

【０７３２】

図９４には、メディアタイプＩＭ４のメモリ情報記録媒体２０を製造すると共に、当該メモリ情報記録媒体２０に対して最新のリストを記録する記録媒体製造装置であるメモリ製造装置６１０の概略構成を示す。なお、記録する最新のリストは、リボケーションリスト又はレジストレーションリストの一方、或いは、リボケーションリスト及びレジストレーションリストの両方の何れであっても良い。この図９４において、図９２と同じ構成要素にはそれぞれ同一の指示符号を付している。

【０７３３】

この図９４に示すメモリ製造装置６１０は、図示しない組立工程により既に組み立てられているメモリ情報記録媒体２０に対して、リストを記録する。但し、メディアタイプＩＭ４であるメモリ情報記録媒体２０は、前述したようにセキュリティモジュール２３がリストを格納するための充分な記憶容量を有する不揮発性メモリ（４４）を備えているため、当該メモリ製造装置６１０は、メモリ情報記録媒体２０のセキュリティモジュール２３内の不揮発性メモリに上記リストを記録する。

【０７３４】

このため、当該メモリ製造装置６１０は、メモリ情報記録媒体２０に信号を送信するためのインターフェース部６１８と、メモリ情報記録媒体２０の入出力端子２４に接続するための入出力端子６０１と、各部を制御する制御部６０５等を備え、さらに、メモリ情報記録媒体２０のＩＤ、秘密鍵、公開鍵証明書、当該媒体２０の製造時点における最新のリスト及びそのバージョンナンバーを予め格納している鍵・リスト記録媒体６０７とそのドライブ部６０６を備えている。なお、この図９４の場合も前記図９２の例と同様に、当該鍵・リスト記録媒体６０７及びドライブ部６０６は外付けの媒体及びドライブであってもよい。上記ＩＤ、秘密鍵、公開鍵証明書、最新のリスト及びバージョンナンバーは、図示しない鍵発行センタにより発行されるものであり、上記内蔵或いは外付けの鍵・リスト記録媒体に予め格納されている。

【０７３５】

上記鍵・リスト記録媒体６０７に格納されている情報は、制御部６０５の制御の元、ドライブ部６０６により読み取られ、インターフェース部６０８及び入出力端子６０１を介して、メモリ情報記録媒体２０に送られる。このときのメモリ情報記録媒体２０では、メモリ製造装置６１０から送られてきた上記ＩＤ、秘密鍵、公開鍵証明書、最新のリスト及びそのバージョンナンバーを、セキュリティモジュール２３の不揮発性メモリ（４４）に記録する。

【０７３６】

またこの図９４の例においても前記図９２の例と同様に、ＩＤ、秘密鍵、公開

鍵証明書、最新のリスト及びそのバージョンナンバーは、上述した内蔵或いは外付けの鍵・リスト記録媒体に予め格納されているものを読み取るだけでなく、例えば鍵発行センタより送られてきたものを外部インターフェース部６０９を介して直接に入手することも可能である。このように、外部インターフェース部６０９を介してＩＤ、秘密鍵、公開鍵証明書、最新のリスト及びそのバージョンナンバーを入手するようにした場合、当該外部インターフェース部６０９を介したＩＤ、秘密鍵、公開鍵証明書、最新のリスト及びそのバージョンナンバーは、制御部６０５からインターフェース部６０８、入出力端子６０１を介して直接メモリ情報記録媒体２０に送られ、セキュリティモジュール２３内の不揮発性メモリ（４４）に記録されることになる。

【０７３７】

図９５には、本発明の記録媒体製造方法として、上記メディアタイプＩＭ４のメモリ情報記録媒体２０を製造すると共に、当該メモリ情報記録媒体２０に対して最新のリストを記録するメモリ製造方法における製造工程の流れを示す。

【０７３８】

図９５において、メモリ製造方法では、先ず、ステップＳ３１０の製造工程として、図示しない組立工程によりメディアタイプＩＭ４のメモリ情報記録媒体２０が組み立てられる。

【０７３９】

次に、メモリ製造方法では、ステップＳ３１１の製造工程として、図９４のメモリ製造装置６１０により、前記ＩＤ、秘密鍵、公開鍵証明書、バージョンナンバーを、メディアタイプＩＭ４であるメモリ情報記録媒体２０のセキュリティモジュール２３内の不揮発性メモリ４４に書き込む。

【０７４０】

次に、メモリ製造方法では、ステップＳ３１２の製造工程として、図９４のメモリ製造装置６１０により、最新のリストをメモリ情報記録媒体２０のセキュリティモジュール２３内の不揮発性メモリ４４に書き込む。

【０７４１】

以上により、メモリ情報記録媒体２０は、最新版のリストをセキュリティモジ

ュール２３の不揮発性メモリ４４に記録した状態で製造工場から出荷されることになる。

【０７４２】

【発明の効果】

以上に説明したように、本発明によれば、記録媒体にセキュリティモジュールを持たせ、記録媒体上に記録されるデータは個々のデータ毎に異なる暗号鍵で暗号化され、暗号鍵はセキュリティモジュールが安全に保管することができる。

【０７４３】

また、本発明において、セキュリティモジュールは、データの記録時及び再生時に、記録再生装置と公開鍵暗号技術を用いた相互認証を行い、相手が正当なライセンスを受けた装置であることを確認した上で、暗号鍵を装置に対して与えることにより、不正な装置にはデータを漏らさないようにすることができる。

【０７４４】

さらに、本発明によれば、信頼できるセンタが発行するリボケーションリスト及び／又はレジストレーションリストを活用することにより、正当な装置だが攻撃されてその装置の秘密が露呈してしまった装置にデータを与えることも防ぐことが可能となる。

【０７４５】

このため、本発明によれば、映画や音楽などの著作権があるデータの不正な（著作権者の意に反する）複製を防ぐことが可能である。

【図面の簡単な説明】

【図１】

本発明を適用した実施の形態としてリスト格納用の不揮発性メモリを備えたセキュリティモジュールを有する光ディスク情報記録媒体の構成を示す図である。

【図２】

光ディスク情報記録媒体のセキュリティモジュールであって、リスト格納用の不揮発性メモリを備えたセキュリティモジュールの一例を示すブロック図である。

【図３】

本発明を適用した実施の形態としてリスト格納用の不揮発性メモリを備えた光ディスク記録再生装置の構成を示すブロック図である。

【図４】

公開鍵証明書の説明に用いる図である。

【図５】

リボケーションリストを説明するための図である。

【図６】

第１の実施の形態の光ディスク情報記録媒体にデータを記録する際の基本的な処理手順の内容を示す図である。

【図７】

第１の実施の形態の光ディスク情報記録媒体にデータを記録する際の詳細な処理手順の内容を示す図である。

【図８】

第１の実施の形態の光ディスク情報記録媒体にデータを記録する際の他の例の処理手順の内容を示す図である。

【図９】

第１の実施の形態の光ディスク情報記録媒体からデータを再生する際の基本的な処理手順の内容を示す図である。

【図１０】

第１の実施の形態の光ディスク情報記録媒体からデータを再生する際の詳細な処理手順の内容を示す図である。

【図１１】

第１の実施の形態の光ディスク情報記録媒体からデータを再生する際の他の例の処理手順の内容を示す図である。

【図１２】

本発明を適用した実施の形態としてリスト格納用の不揮発性メモリを備えたセキュリティモジュールを有するメモリ情報記録媒体の構成を示す図である。

【図１３】

メモリ情報記録媒体のセキュリティモジュールであって、リスト格納用の不揮発性メモリを備えたセキュリティモジュールの一例を示すブロック図である。

【図１４】

本発明を適用した実施の形態のメモリ記録再生装置の構成を示すブロック図である。

【図１５】

第２の実施の形態のメモリ情報記録媒体にデータを記録する際の基本的な処理手順の内容を示す図である。

【図１６】

第２の実施の形態のメモリ情報記録媒体にデータを記録する際の詳細な処理手順の内容を示す図である。

【図１７】

第２の実施の形態のメモリ情報記録媒体にデータを記録する際の他の例の処理手順の内容を示す図である。

【図１８】

第２の実施の形態のメモリ情報記録媒体にデータを記録する際のさらに他の例の処理手順の内容を示す図である。

【図１９】

第２の実施の形態のメモリ情報記録媒体からデータを再生する際の基本的な処理手順の内容を示す図である。

【図２０】

第２の実施の形態のメモリ情報記録媒体からデータを再生する際の詳細な処理手順の内容を示す図である。

【図２１】

第２の実施の形態のメモリ情報記録媒体からデータを再生する際の他の例の処理手順の内容を示す図である。

【図２２】

第２の実施の形態のメモリ情報記録媒体からデータを再生する際のさらに他の

例の処理手順の内容を示す図である。

【図２３】

レジストレーションリストを説明するための図である。

【図２４】

第３の実施の形態の光ディスク情報記録媒体にデータを記録する際の基本的な処理手順の内容を示す図である。

【図２５】

第３の実施の形態の光ディスク情報記録媒体にデータを記録する際の詳細な処理手順の内容を示す図である。

【図２６】

第３の実施の形態の光ディスク情報記録媒体にデータを記録する際の他の例の処理手順の内容を示す図である。

【図２７】

第３の実施の形態の光ディスク情報記録媒体からデータを再生する際の基本的な処理手順の内容を示す図である。

【図２８】

第３の実施の形態の光ディスク情報記録媒体からデータを再生する際の詳細な処理手順の内容を示す図である。

【図２９】

第３の実施の形態の光ディスク情報記録媒体からデータを再生する際の他の例の処理手順の内容を示す図である。

【図３０】

第４の実施の形態のメモリ情報記録媒体にデータを記録する際の基本的な処理手順の内容を示す図である。

【図３１】

第４の実施の形態のメモリ情報記録媒体にデータを記録する際の詳細な処理手順の内容を示す図である。

【図３２】

第４の実施の形態のメモリ情報記録媒体にデータを記録する際の他の例の処理

手順の内容を示す図である。

【図３３】

第２の実施の形態のメモリ情報記録媒体にデータを記録する際のさらに他の例の処理手順の内容を示す図である。

【図３４】

第４の実施の形態のメモリ情報記録媒体からデータを再生する際の基本的な処理手順の内容を示す図である。

【図３５】

第４の実施の形態のメモリ情報記録媒体からデータを再生する際の詳細な処理手順の内容を示す図である。

【図３６】

第４の実施の形態のメモリ情報記録媒体からデータを再生する際の他の例の処理手順の内容を示す図である。

【図３７】

第４の実施の形態のメモリ情報記録媒体からデータを再生する際のさらに他の例の処理手順の内容を示す図である。

【図３８】

リボケーションリスト／レジストレーションリストを説明するための図である。

【図３９】

第５の実施の形態の光ディスク情報記録媒体にデータを記録する際の基本的な処理手順の内容を示す図である。

【図４０】

第５の実施の形態の光ディスク情報記録媒体にデータを記録する際の詳細な処理手順の内容を示す図である。

【図４１】

第５の実施の形態の光ディスク情報記録媒体にデータを記録する際の他の例の処理手順の内容を示す図である。

【図４２】

第５の実施の形態の光ディスク情報記録媒体からデータを再生する際の基本的な処理手順の内容を示す図である。

【図４３】

第５の実施の形態の光ディスク情報記録媒体からデータを再生する際の詳細な処理手順の内容を示す図である。

【図４４】

第５の実施の形態の光ディスク情報記録媒体からデータを再生する際の他の例の処理手順の内容を示す図である。

【図４５】

第６の実施の形態のメモリ情報記録媒体にデータを記録する際の基本的な処理手順の内容を示す図である。

【図４６】

第６の実施の形態のメモリ情報記録媒体にデータを記録する際の詳細な処理手順の内容を示す図である。

【図４７】

第６の実施の形態のメモリ情報記録媒体にデータを記録する際の他の例の処理手順の内容を示す図である。

【図４８】

第６の実施の形態のメモリ情報記録媒体にデータを記録する際のさらに他の例の処理手順の内容を示す図である。

【図４９】

第６の実施の形態のメモリ情報記録媒体からデータを再生する際の基本的な処理手順の内容を示す図である。

【図５０】

第６の実施の形態のメモリ情報記録媒体からデータを再生する際の詳細な処理手順の内容を示す図である。

【図５１】

第６の実施の形態のメモリ情報記録媒体からデータを再生する際の他の例の処

理手順の内容を示す図である。

【図５２】

第６の実施の形態のメモリ情報記録媒体からデータを再生する際のさらに他の例の処理手順の内容を示す図である。

【図５３】

リスト格納用の不揮発性メモリを備えないセキュリティモジュールを有する光ディスク情報記録媒体の構成を示す図である。

【図５４】

光ディスク情報記録媒体のセキュリティモジュールであって、リスト格納用の不揮発性メモリを備えないセキュリティモジュールの一例を示すブロック図である。

【図５５】

リスト格納用の不揮発性メモリを備えないセキュリティモジュールを有するメモリ情報記録媒体の構成を示す図である。

【図５６】

メモリ情報記録媒体のセキュリティモジュールであって、リスト格納用の不揮発性メモリを備えないセキュリティモジュールの一例を示すブロック図である。

【図５７】

第７の実施の形態の光ディスク情報記録媒体とその光ディスク記録再生装置の構成を示すブロック図である。

【図５８】

第７の実施の形態の光ディスク情報記録媒体にデータを記録する際の基本的な処理手順の内容を示す図である。

【図５９】

第７の実施の形態の光ディスク情報記録媒体にデータを記録する際の詳細な処理手順の内容を示す図である。

【図６０】

第７の実施の形態の光ディスク情報記録媒体からデータを再生する際の基本的な処理手順の内容を示す図である。

【図６１】

第８の実施の形態の光ディスク情報記録媒体とその光ディスク記録再生装置の構成を示すブロック図である。

【図６２】

第８の実施の形態の光ディスク情報記録媒体にデータを記録する際の基本的な処理手順の内容を示す図である。

【図６３】

第８の実施の形態の光ディスク情報記録媒体にデータを記録する際の詳細な処理手順の内容を示す図である。

【図６４】

第８の実施の形態の光ディスク情報記録媒体からデータを再生する際の基本的な処理手順の内容を示す図である。

【図６５】

第９の実施の形態の光ディスク情報記録媒体とその光ディスク記録再生装置の構成を示すブロック図である。

【図６６】

第９の実施の形態の光ディスク情報記録媒体にデータを記録する際の基本的な処理手順の内容を示す図である。

【図６７】

第９の実施の形態の光ディスク情報記録媒体にデータを記録する際の詳細な処理手順の内容を示す図である。

【図６８】

第９の実施の形態の光ディスク情報記録媒体からデータを再生する際の基本的な処理手順の内容を示す図である。

【図６９】

第１０の実施の形態のメモリ情報記録媒体とそのメモリ記録再生装置の構成を示すブロック図である。

【図７０】

第１０の実施の形態のメモリ情報記録媒体にデータを記録する際の基本的な処

理手順の内容を示す図である。

【図７１】

第１０の実施の形態のメモリ情報記録媒体にデータを記録する際の詳細な処理手順の内容を示す図である。

【図７２】

第１０の実施の形態のメモリ情報記録媒体からデータを再生する際の基本的な処理手順の内容を示す図である。

【図７３】

第１１の実施の形態のメモリ情報記録媒体とそのメモリ記録再生装置の構成を示すブロック図である。

【図７４】

第１１の実施の形態のメモリ情報記録媒体にデータを記録する際の基本的な処理手順の内容を示す図である。

【図７５】

第１１の実施の形態のメモリ情報記録媒体にデータを記録する際の詳細な処理手順の内容を示す図である。

【図７６】

第１１の実施の形態のメモリ情報記録媒体からデータを再生する際の基本的な処理手順の内容を示す図である。

【図７７】

第１２の実施の形態のメモリ情報記録媒体とそのメモリ記録再生装置の構成を示すブロック図である。

【図７８】

第１２の実施の形態のメモリ情報記録媒体にデータを記録する際の基本的な処理手順の内容を示す図である。

【図７９】

第１２の実施の形態のメモリ情報記録媒体にデータを記録する際の詳細な処理手順の内容を示す図である。

【図８０】

第１２の実施の形態のメモリ情報記録媒体からデータを再生する際の基本的な処理手順の内容を示す図である。

【図８１】

メディアタイプＩＭ１に相当する光ディスク情報記録媒体のセキュリティモジュールにおける処理の流れを示すフローチャートである。

【図８２】

メディアタイプＩＭ２に相当する光ディスク情報記録媒体のセキュリティモジュールにおける処理の流れを示すフローチャートである。

【図８３】

メディアタイプＩＭ３に相当するメモリ情報記録媒体のセキュリティモジュールにおける処理の流れを示すフローチャートである。

【図８４】

メディアタイプＩＭ４に相当するメモリ情報記録媒体のセキュリティモジュールにおける処理の流れを示すフローチャートである。

【図８５】

デバイスタイプＤｅｖ１及びＤｅｖ３の記録再生装置の処理の流れを示すフローチャートである。

【図８６】

デバイスタイプＤｅｖ２及びＤｅｖ４の記録再生装置の処理の前半部分の流れを示すフローチャートである。

【図８７】

デバイスタイプＤｅｖ２及びＤｅｖ４の記録再生装置の処理の後半部分の流れを示すフローチャートである。

【図８８】

メディアタイプＩＭ１の光ディスク情報記録媒体に最新のリストを記録する光ディスク製造装置の概略構成を示すブロック図である。

【図８９】

メディアタイプＩＭ１の光ディスク情報記録媒体に最新のリストを記録する光

ディスク製造工程の流れを示すフローチャートである。

【図９０】

メディアタイプＩＭ２の光ディスク情報記録媒体に最新のリストを記録する光ディスク製造装置の概略構成を示すブロック図である。

【図９１】

メディアタイプＩＭ２の光ディスク情報記録媒体に最新のリストを記録する光ディスク製造工程の流れを示すフローチャートである。

【図９２】

メディアタイプＩＭ３のメモリ情報記録媒体に最新のリストを記録するメモリ製造装置の概略構成を示すブロック図である。

【図９３】

メディアタイプＩＭ３のメモリ情報記録媒体に最新のリストを記録するメモリ製造工程の流れを示すフローチャートである。

【図９４】

メディアタイプＩＭ４のメモリ情報記録媒体に最新のリストを記録するメモリ製造装置の概略構成を示すブロック図である。

【図９５】

メディアタイプＩＭ４のメモリ情報記録媒体に最新のリストを記録するメモリ製造工程の流れを示すフローチャートである。

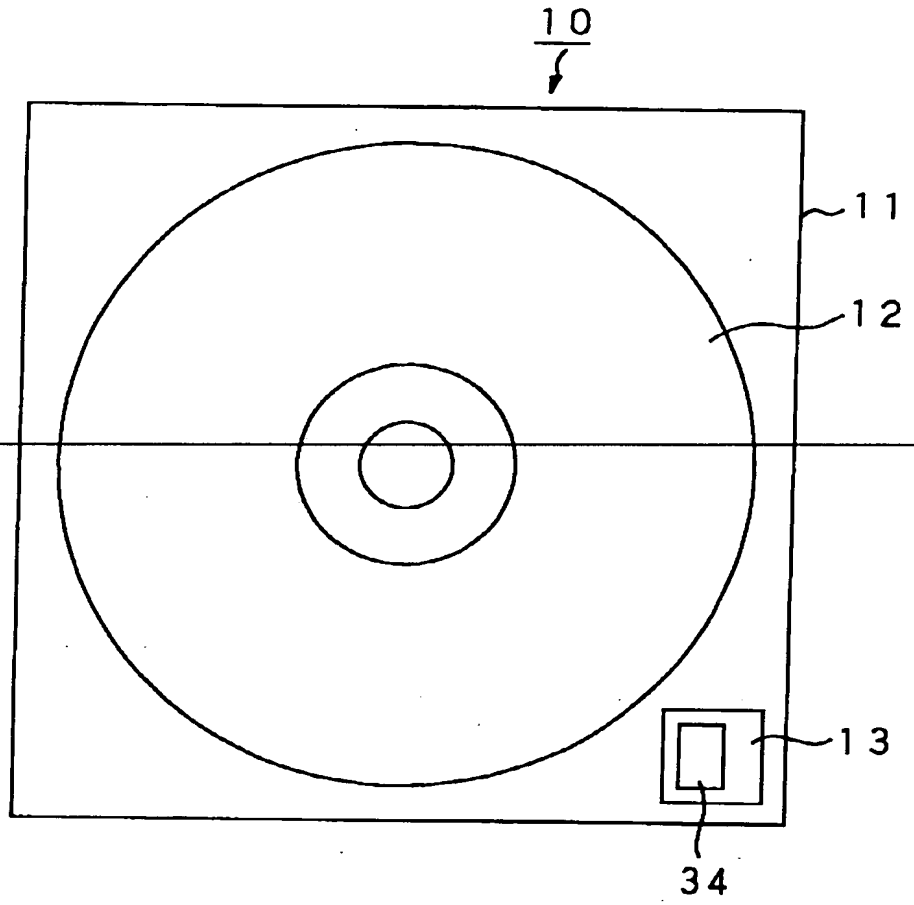
【符号の説明】

１０，５０　光ディスク情報記録媒体、１１　カートリッジ、１２　光ディスク、１３，２３，５３，６３　セキュリティモジュール、３１　インターフェース部、３２　演算部、３３　乱数発生部、３４　不揮発性メモリ、３５　制御部、３４，４４，１１０，２１０　不揮発性メモリ、１００，３００　光ディスク記録再生装置、１０１　スピンドルモータ、１０２　光学ヘッド、１０３　サーボ回路、１０４　記録／再生回路、１０５　制御部、１０６　入力部、１０７　乱数発生部、１０８　インターフェース部、１０９　演算部１０９、２０，６０　メモリ情報記録媒体、２１　カートリッジ、２４　入出力端子、４１　外部インターフェース部、４２　演算部、４３　乱数発生部、４５　制御部、４６　記

録媒体インターフェース部、２００，４００　メモリ記録再生装置、２０１　入出力端子、２０５　制御部、２０６　入力部、２０７　乱数発生部、２０８　インターフェース部、２０９　演算部、　５００，５１０　光ディスク製造装置、６００，６１０　メモリ製造装置

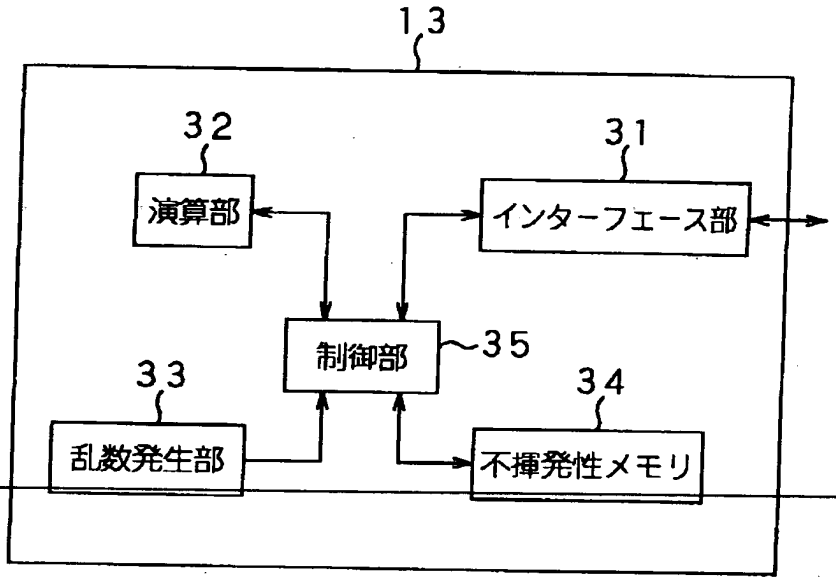
【書類名】　　図面

【図１】

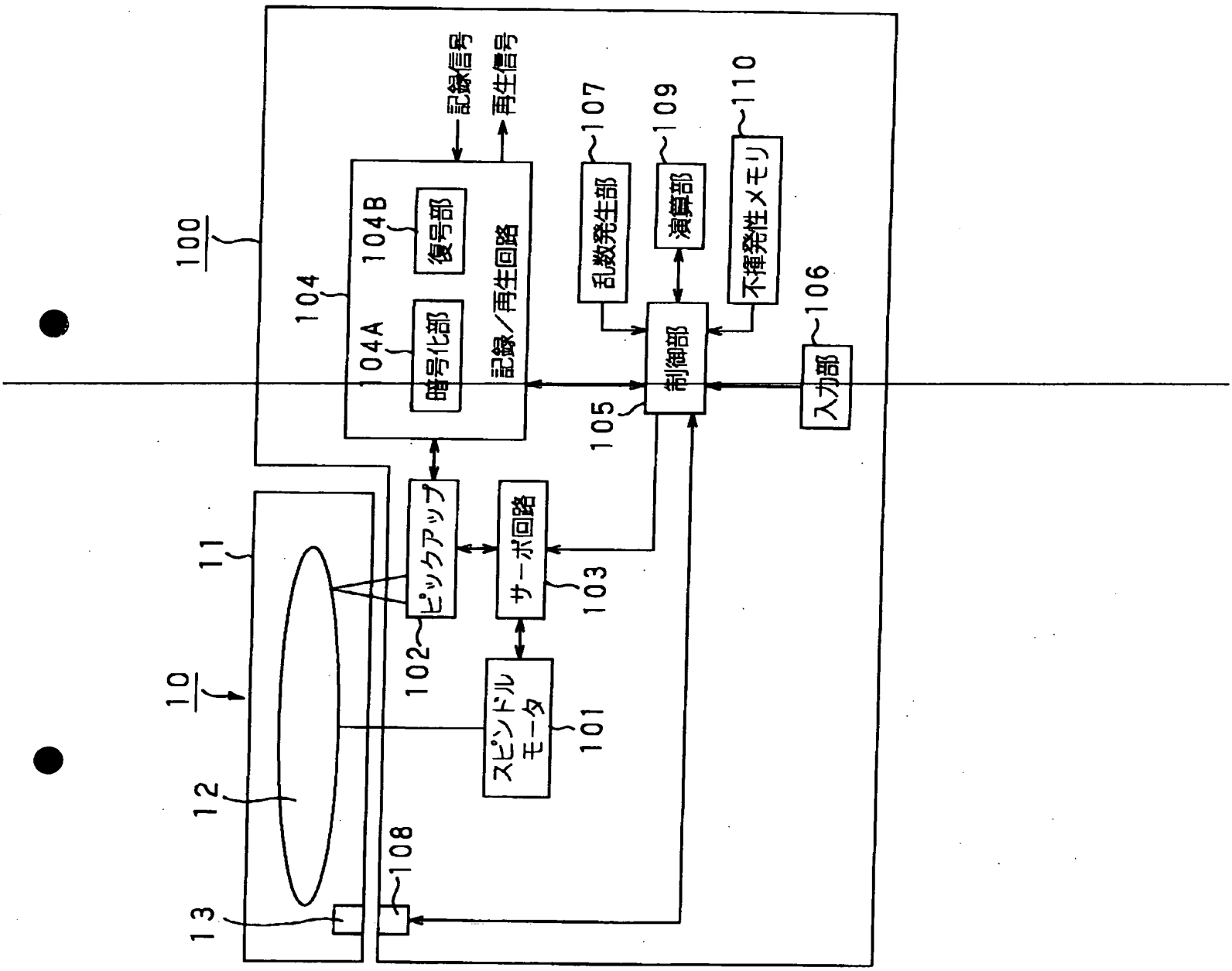


出証特２０００－３０５００８５

【図２】



【図３】


100
104
104A
暗号化部
104B
復号部
記録／再生回路
記録信号
再生信号
乱数発生部
107
演算部
109
不揮発性メモリ
110
制御部
105
入力部
106
ピックアップ
102
サーボ回路
103
スピンドルモータ
101
10
11
12
13
108

【図４】

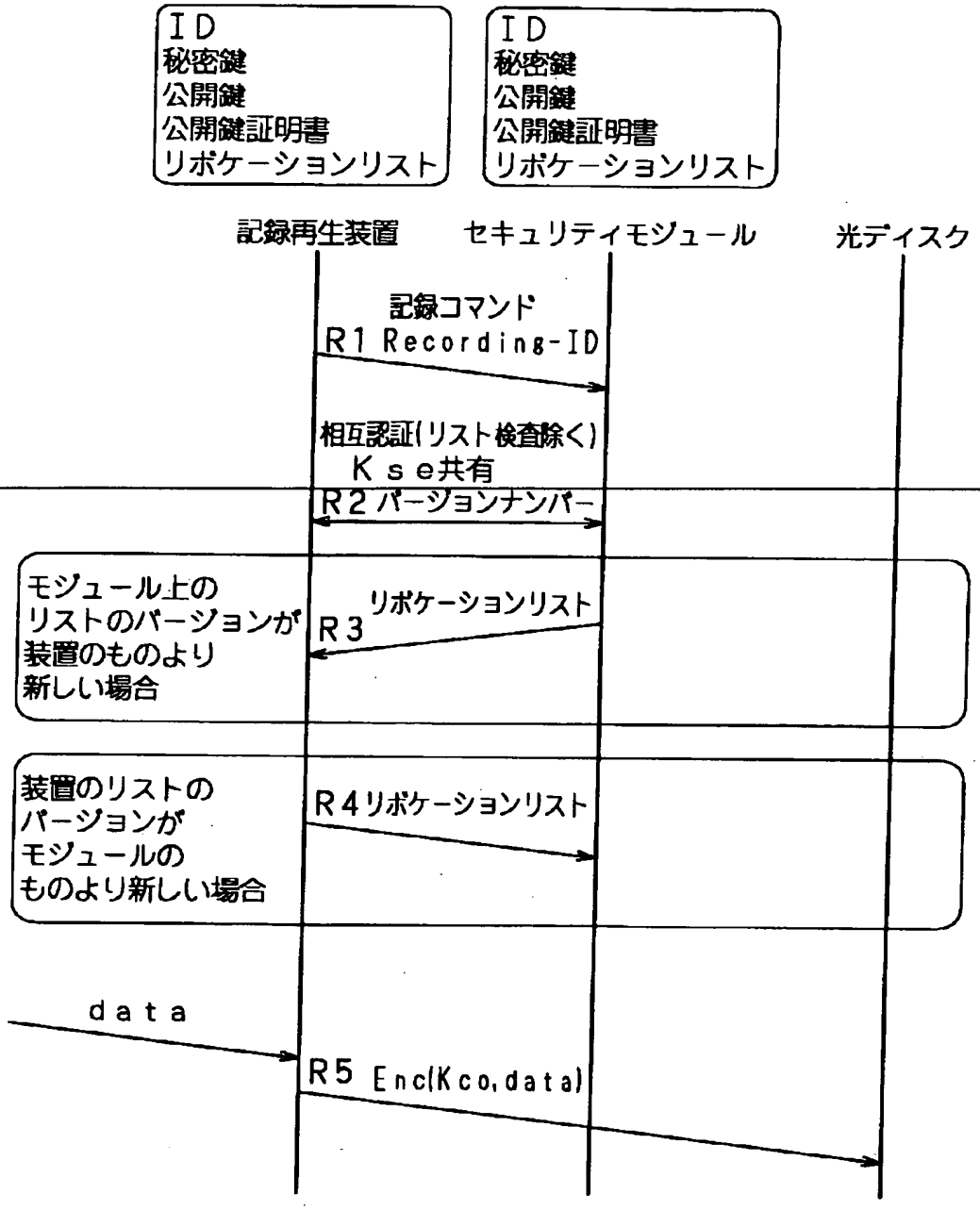
エンティティＩＤ
エンティティタイプ
エンティティ公開鍵
ＴＣのデジタル署名

【図５】

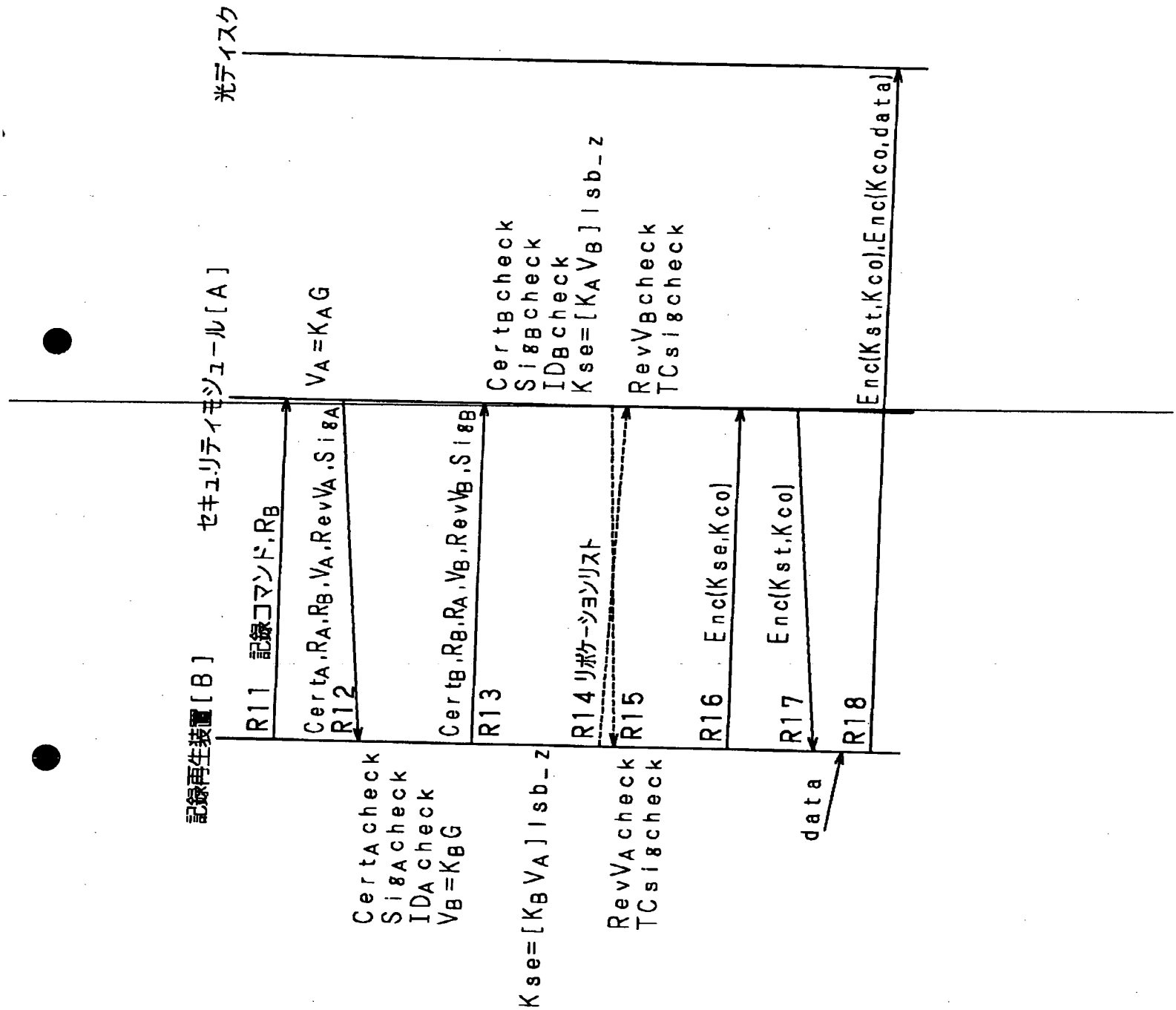
リポケーションリスト

バージョンナンバー
リポークされる機器または媒体のＩＤ
・・・・・・
ＴＣのデジタル署名

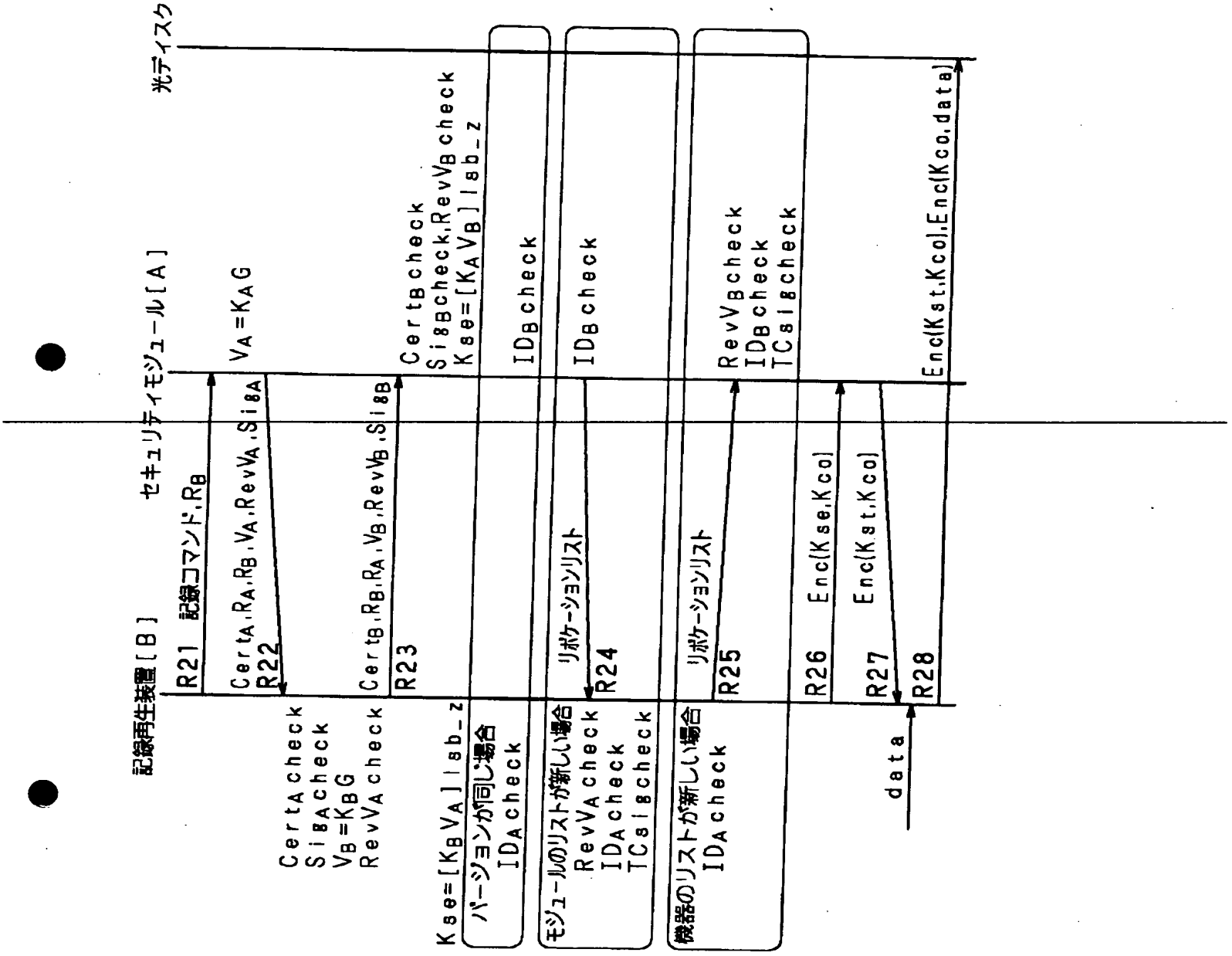
【図６】


ＩＤ
秘密鍵
公開鍵
公開鍵証明書
リボケーションリスト
ＩＤ
秘密鍵
公開鍵
公開鍵証明書
リボケーションリスト
記録再生装置
セキュリティモジュール
光ディスク
記録コマンド
R1 Recording-ID
相互認証(リスト検査除く)
Ｋｓｅ共有
R2 バージョンナンバー
モジュール上の
リストのバージョンが
装置のものより
新しい場合
リボケーションリスト
R3
装置のリストの
バージョンが
モジュールの
ものより新しい場合
R4 リボケーションリスト
ｄａｔａ
R5 Enc(Kco,data)

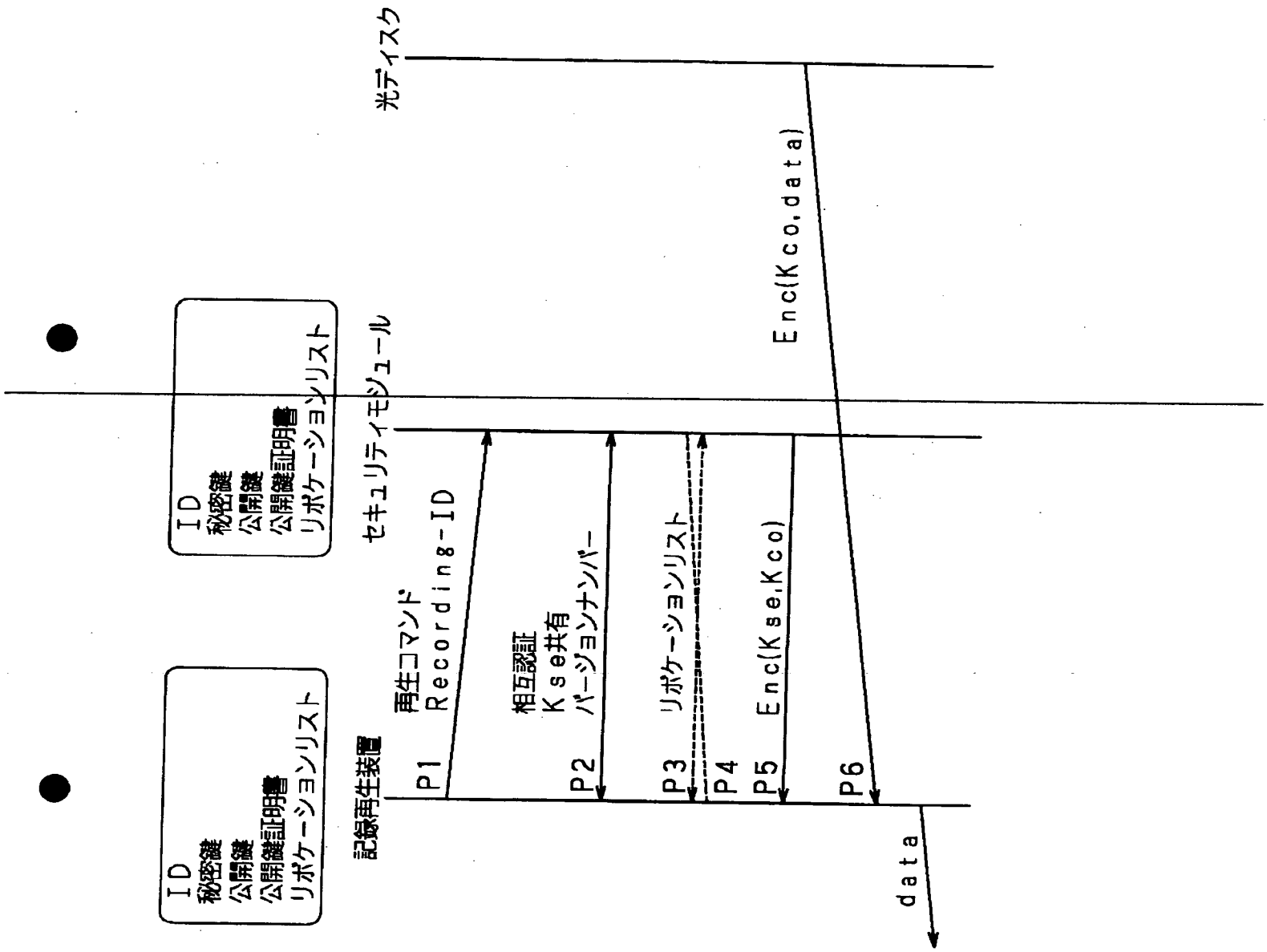
【図７】


光ディスク
セキュリティモジュール[A]
記録再生装置[B]
R11 記録コマンド,RB
VA=KAG
CertA,RA,RB,VA,RevVA,SigA
R12
CertB,RB,RA,VB,RevVB,SigB
R13
CertBcheck
SigBcheck
IDBcheck
Kse=[KAVB]lsb_z
R14 リボケーションリスト
R15
RevVBcheck
TCsigcheck
R16 Enc(Kse,Kcol)
R17 Enc(Kst,Kcol)
R18 Enc(Kst,Kco),Enc(Kco,data)
CertAcheck
SigAcheck
IDAcheck
VB=KBG
Kse=[KBVA]lsb_z
RevVAcheck
TCsigcheck
data

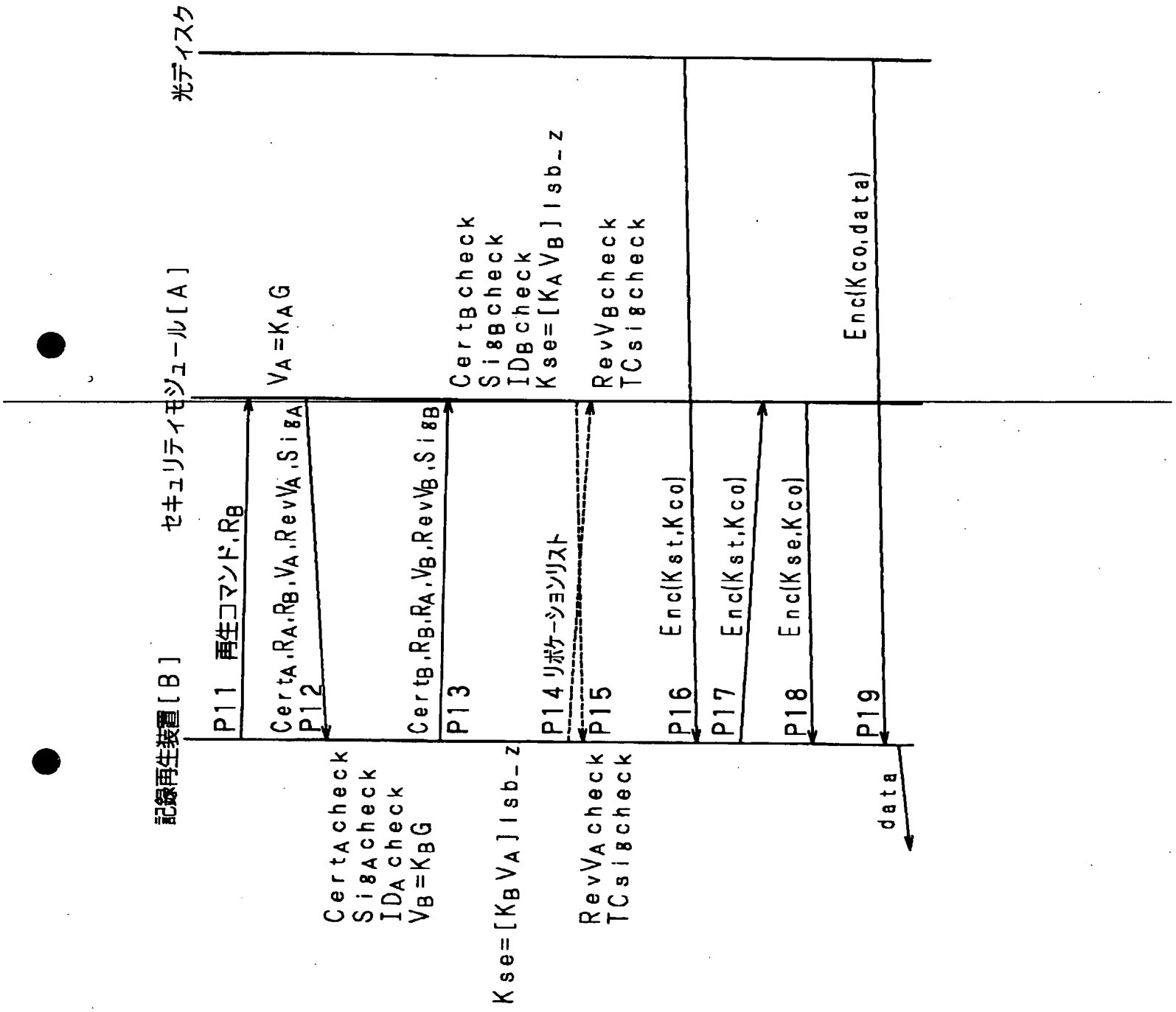
【図８】


記録再生装置[B]
セキュリティモジュール[A]
光ディスク
R21 記録コマンド,RB
CertA,RA,RB,VA,RevVA,SigA
R22
CertB,RB,RA,VB,RevVB,SigB
R23
Kse=[KBVA]lsb_z
R24
R25
R26 Enc(Kse,Kco)
R27 Enc(Kst,Kco)
R28
data
VA=KAG
CertB check
SigB check,RevVB check
Kse=[KAVB]lsb_z
IDB check
CertA check
SigA check
VB=KBG
RevVA check
パージョンが同じ場合
IDA check
リボケーションリスト
モジュール1のリストが新しい場合
RevVA check
IDA check
TCsig check
リボケーションリスト
機器のリストが新しい場合
IDA check
RevVB check
IDB check
TCsig check
Enc(Kst,Kco),Enc(Kco,data)

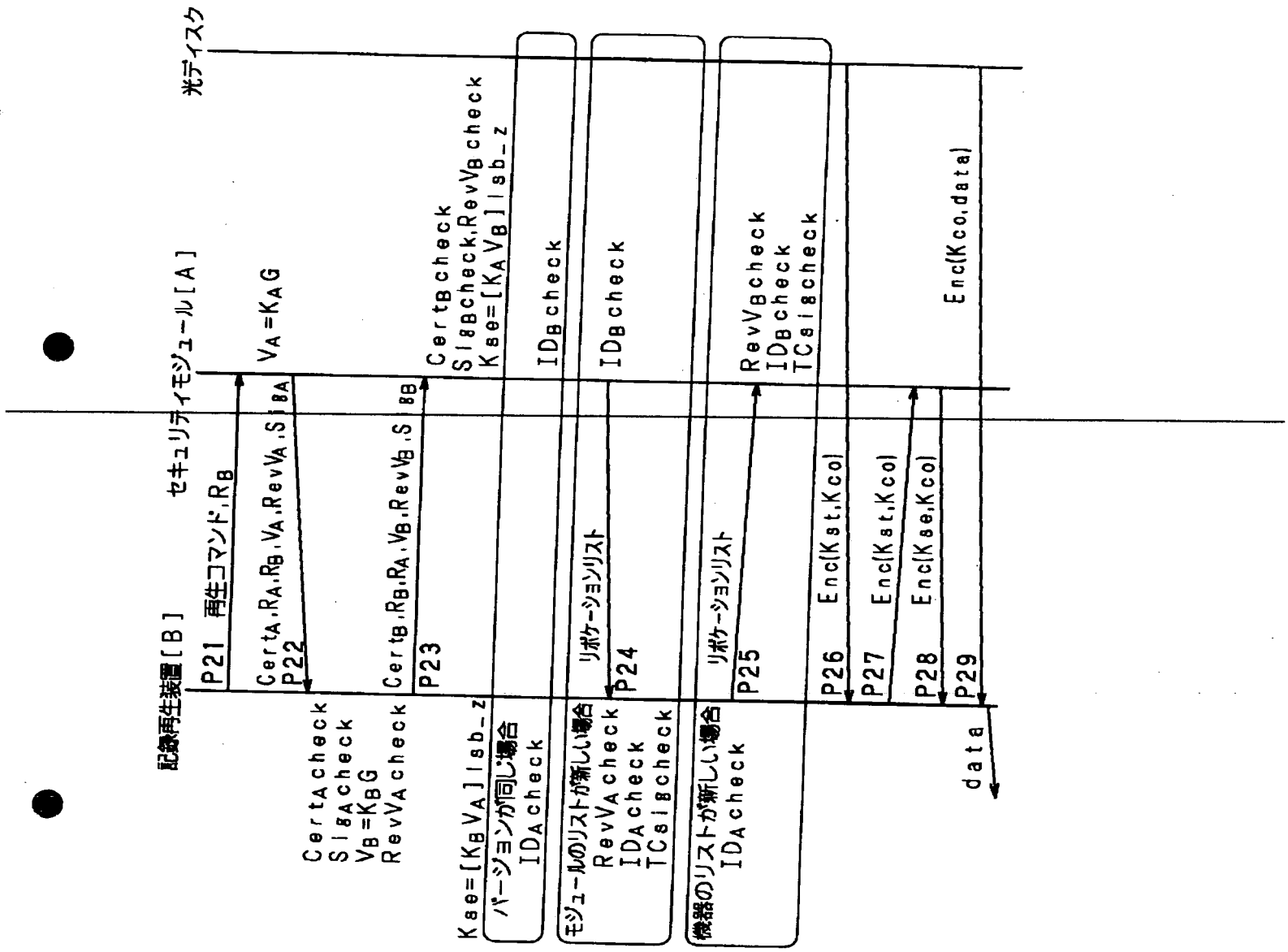
【図９】


光ディスク
ID
秘密鍵
公開鍵
公開鍵証明書
リボケーションリスト
セキュリティモジュール
Enc(Kco,data)
ID
秘密鍵
公開鍵
公開鍵証明書
リボケーションリスト
記録再生装置
再生コマンド
Recording-ID
P1
相互認証
Kse共有
バージョンナンバー
P2
リボケーションリスト
P3
P4
Enc(Kse,Kco)
P5
P6
data

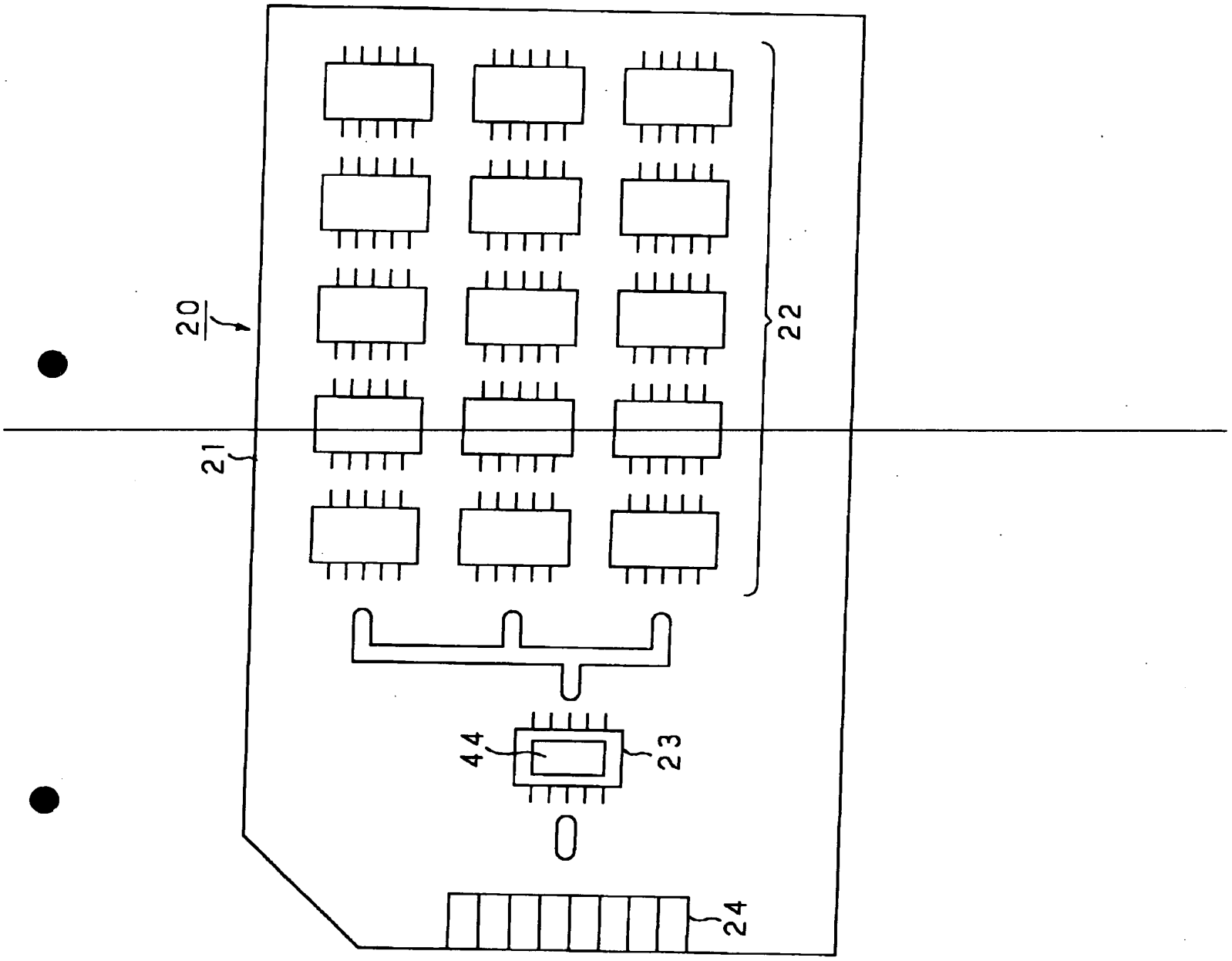
【図１０】


光ディスク
セキュリティモジュール[A]
記録再生装置[B]
P11 再生コマンド,RB
CertA,RA,RB,VA,RevVA,SigA
P12
CertB,RB,RA,VB,RevVB,SigB
P13
P14 リボケーションリスト
P15
P16 Enc(Kst,Kcol)
P17 Enc(Kst,Kcol)
P18 Enc(Kse,Kcol)
P19
data
VA=KAG
CertB check
SigB check
IDB check
Kse=[KAVB]lsb_z
RevVB check
TCsig check
Enc(Kco,data)
CertA check
SigA check
IDA check
VB=KBG
Kse=[KBVA]lsb_z
RevVA check
TCsig check

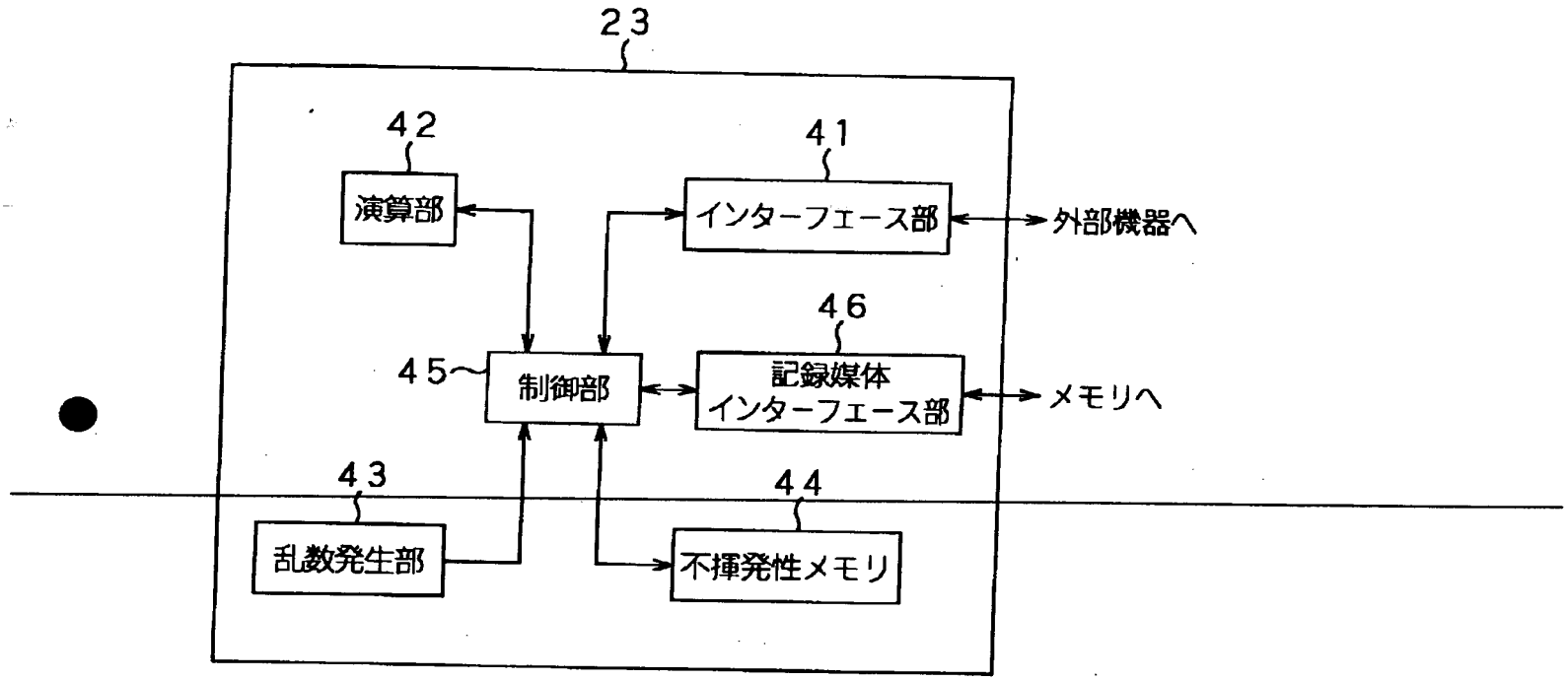
【図１１】


光ディスク
セキュリティモジュール[A]
記録再生装置[B]
P21 再生コマンド,RB
VA=KAG
CertA,RA,RB,VA,RevVA,SigA
P22
CertB,RB,RA,VB,RevVB,SigB
P23
CertBcheck
SigBcheck,RevVBcheck
Kse=[KAVB]Isb_z
IDBcheck
IDBcheck
RevVBcheck
IDBcheck
TCsigcheck
Enc(Kco,data)
CertAcheck
SigAcheck
VB=KBG
RevVAcheck
Kse=[KBVA]Isb_z
バージョンが同じ場合
IDAcheck
モジュールのリストが新しい場合
RevVAcheck
IDAcheck
TCsigcheck
リボケーションリスト
P24
機器のリストが新しい場合
IDAcheck
リボケーションリスト
P25
P26 Enc(Kst,Kcol)
P27 Enc(Kst,Kcol)
P28 Enc(Kse,Kcol)
P29
data

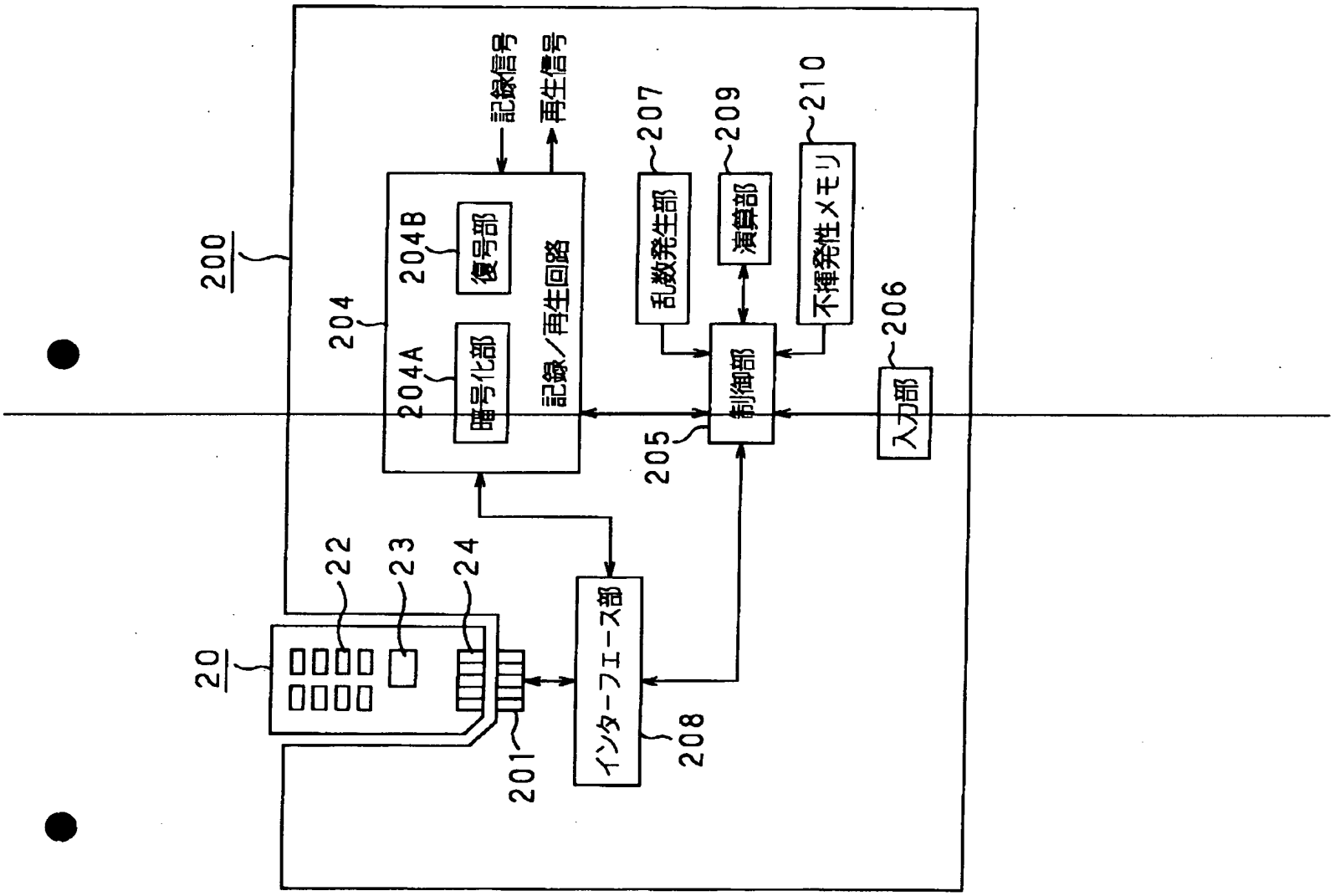
【図１２】



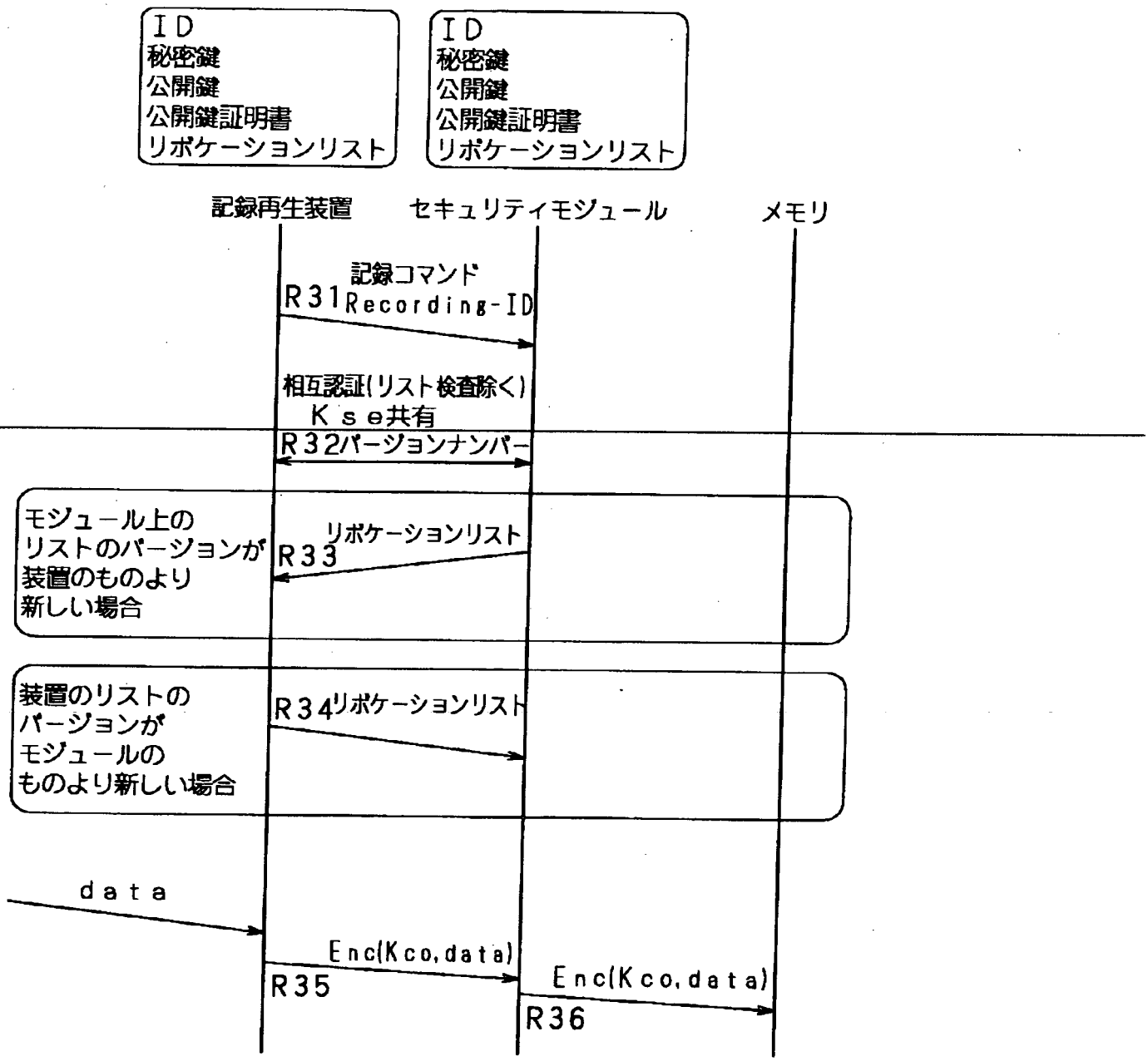
【図１３】


23
42
演算部
41
インターフェース部
外部機器へ
46
45
制御部
記録媒体
インターフェース部
メモリへ
43
乱数発生部
44
不揮発性メモリ

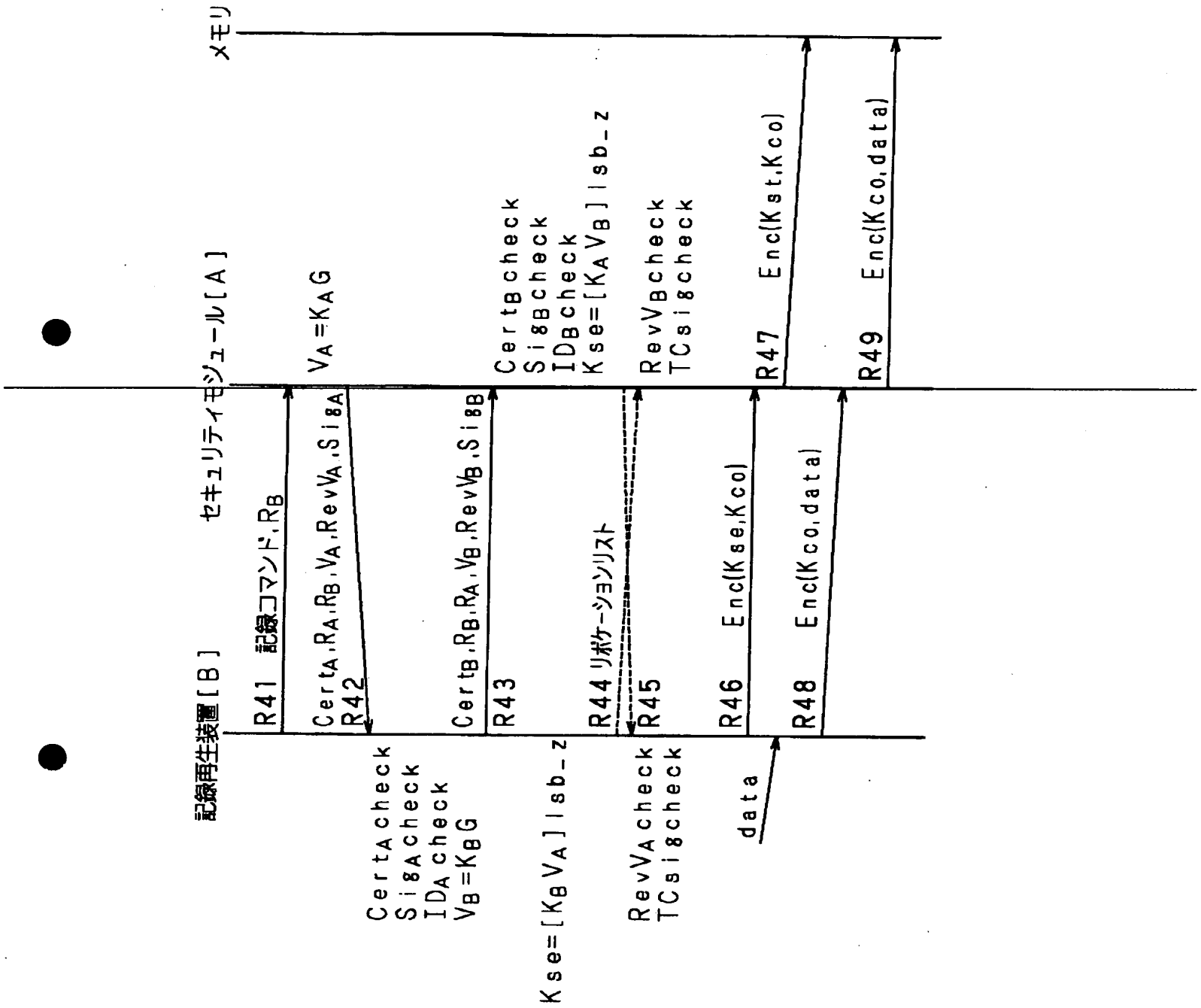
【図１４】


200
記録信号
再生信号
204
204B
復号部
204A
暗号化部
記録／再生回路
乱数発生部
207
演算部
209
不揮発性メモリ
210
制御部
205
入力部
206
20
22
23
24
インターフェース部
208
201

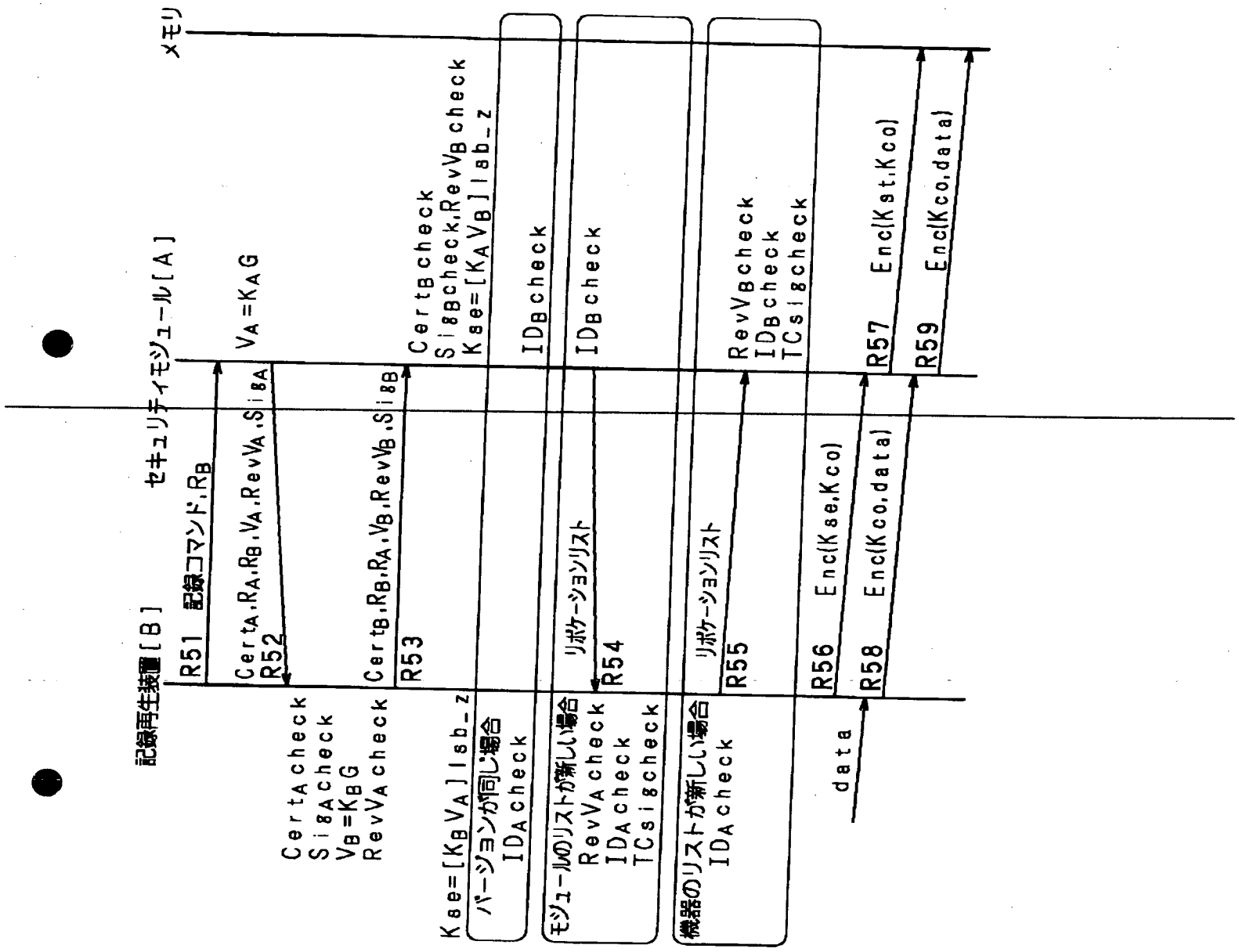
【図１５】


ＩＤ
秘密鍵
公開鍵
公開鍵証明書
リボケーションリスト
ＩＤ
秘密鍵
公開鍵
公開鍵証明書
リボケーションリスト
記録再生装置
セキュリティモジュール
メモリ
記録コマンド
R31 Recording-ID
相互認証(リスト検査除く)
Ｋｓｅ共有
R32バージョンナンバー
モジュール上の
リストのバージョンが
装置のものより
新しい場合
リボケーションリスト
R33
装置のリストの
バージョンが
モジュールの
ものより新しい場合
R34リボケーションリスト
ｄａｔａ
Enc(Kco,data)
R35
Enc(Kco,data)
R36

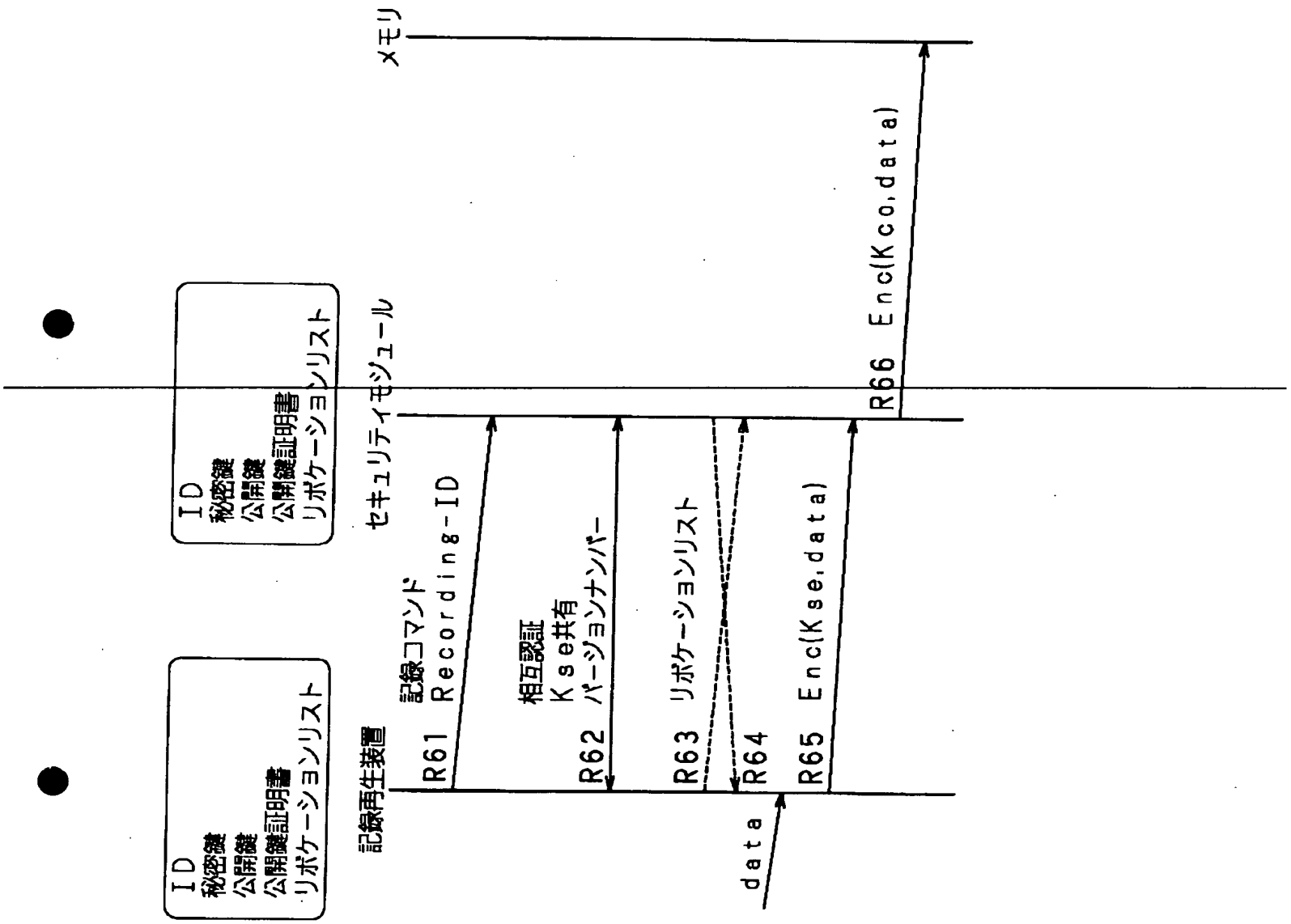
【図１６】


メモリ
セキュリティモジュール[A]
記録再生装置[B]
R41 記録コマンド,RB
VA=KAG
CertA,RA,RB,VA,RevVA,SigA
R42
CertA check
SigA check
IDA check
VB=KBG
CertB,RB,RA,VB,RevVB,SigB
R43
CertB check
SigB check
IDB check
Kse=[KAVB]lsb_z
R44 リボケーションリスト
R45
RevVB check
TCsig check
R46 Enc(Kse,Kco)
Kse=[KBVA]lsb_z
RevVA check
TCsig check
data
R47 Enc(Kst,Kco)
R48 Enc(Kco,data)
R49 Enc(Kco,data)

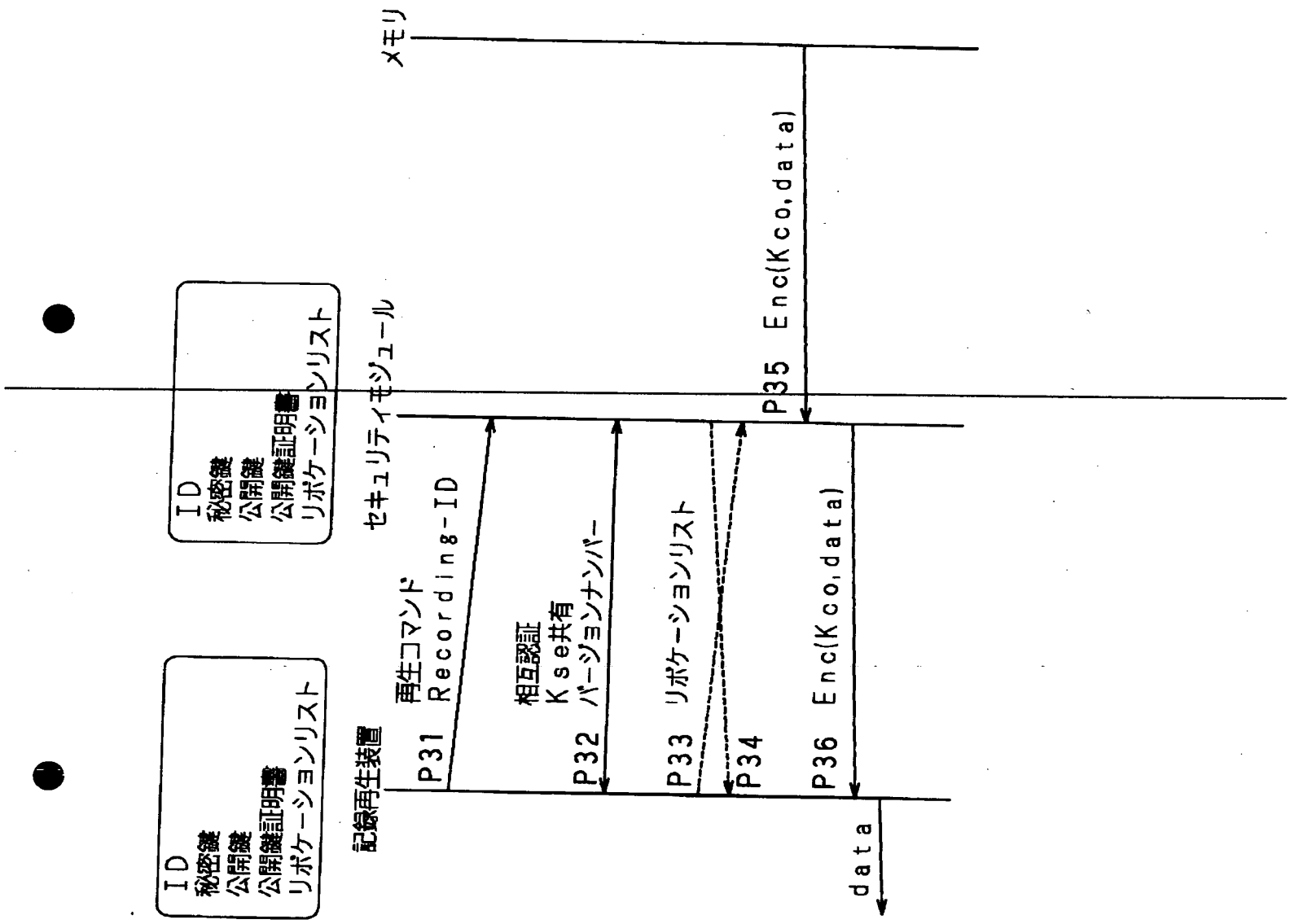
【図１７】


記録再生装置[B]
セキュリティモジュール[A]
メモリ
R51 記録コマンド,RB
VA=KAG
R52
CertA,RA,RB,VA,RevVA,SigA
CertB,RB,RA,VB,RevVB,SigB
R53
CertB check
SigBcheck,RevVB check
Kse=[KAVB]lsb_z
IDB check
R54
リボケーションリスト
IDB check
R55
リボケーションリスト
RevVB check
IDB check
TCsig check
R56 Enc(Kse,Kco)
R57 Enc(Kst,Kco)
R58 Enc(Kco,data)
R59 Enc(Kco,data)
data
CertA check
SigA check
VB=KBG
RevVA check
Kse=[KBVA]lsb_z
バージョンが同じ場合
IDA check
モジュールのリストが新しい場合
RevVA check
IDA check
TCsig check
機器のリストが新しい場合
IDA check

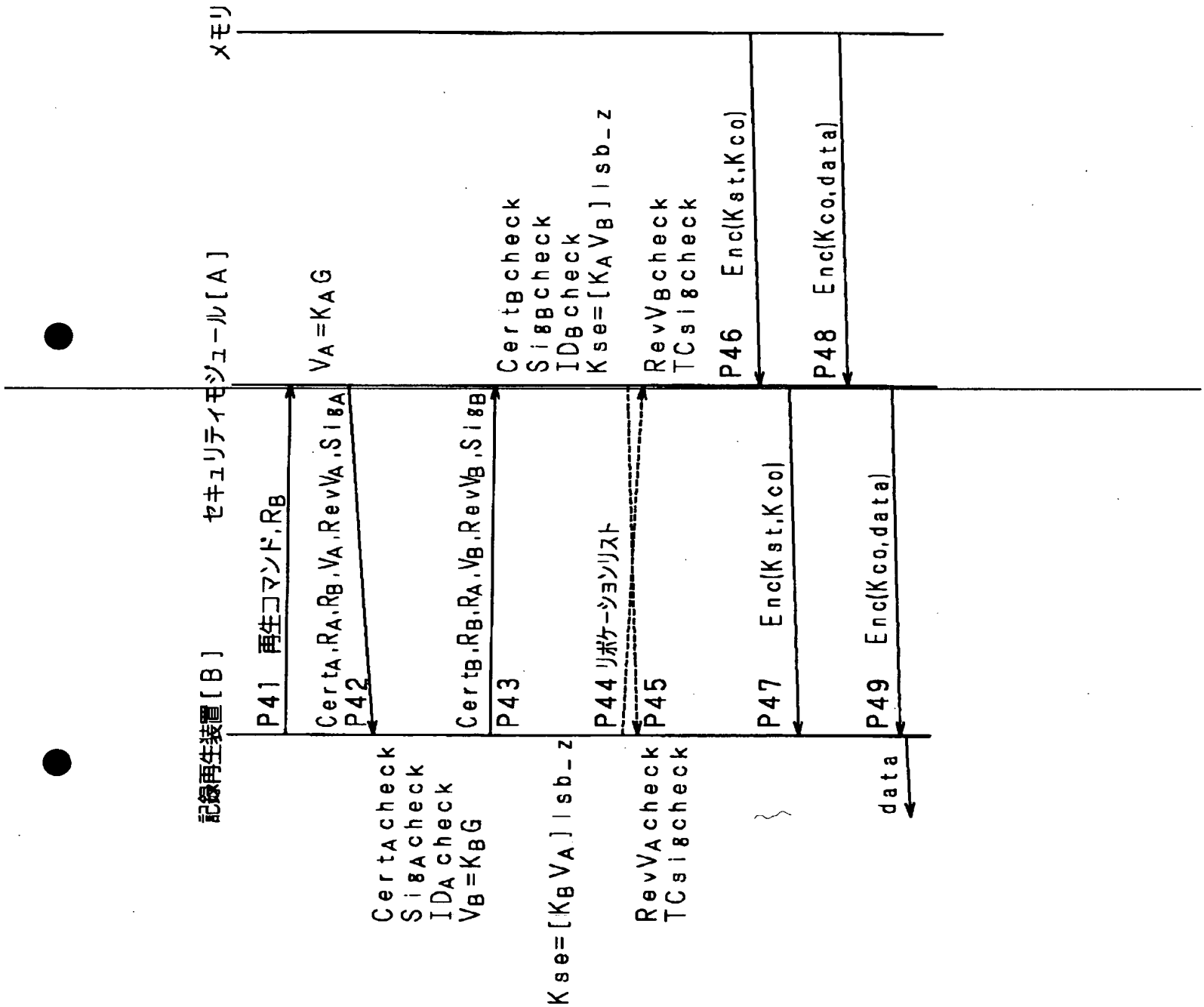
【図１８】


メモリ
セキュリティモジュール
記録再生装置
ID
秘密鍵
公開鍵
公開鍵証明書
リボケーションリスト
ID
秘密鍵
公開鍵
公開鍵証明書
リボケーションリスト
記録コマンド
Recording-ID
R61
相互認証
Kse共有
バージョンナンバー
R62
R63 リボケーションリスト
R64
R65 Enc(Kse,data)
R66 Enc(Kco,data)
data

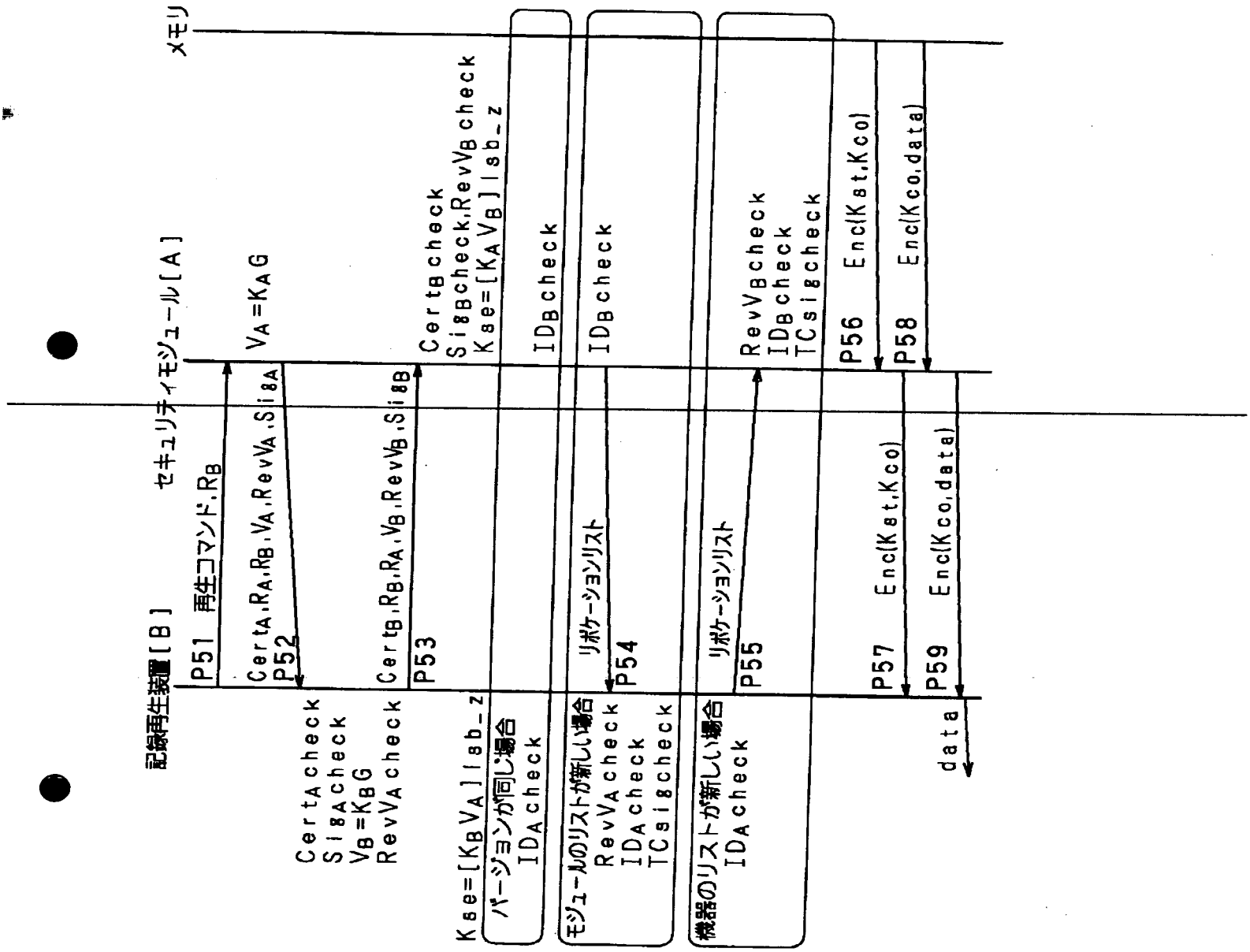
【図１９】


メモリ
ID
秘密鍵
公開鍵
公開鍵証明書
リボケーションリスト
セキュリティモジュール
P35 Enc(Kco,data)
ID
秘密鍵
公開鍵
公開鍵証明書
リボケーションリスト
記録再生装置
再生コマンド
Recording-ID
P31
相互認証
Kse共有
バージョンナンバー
P32
リボケーションリスト
P33
P34
P36 Enc(Kco,data)
data

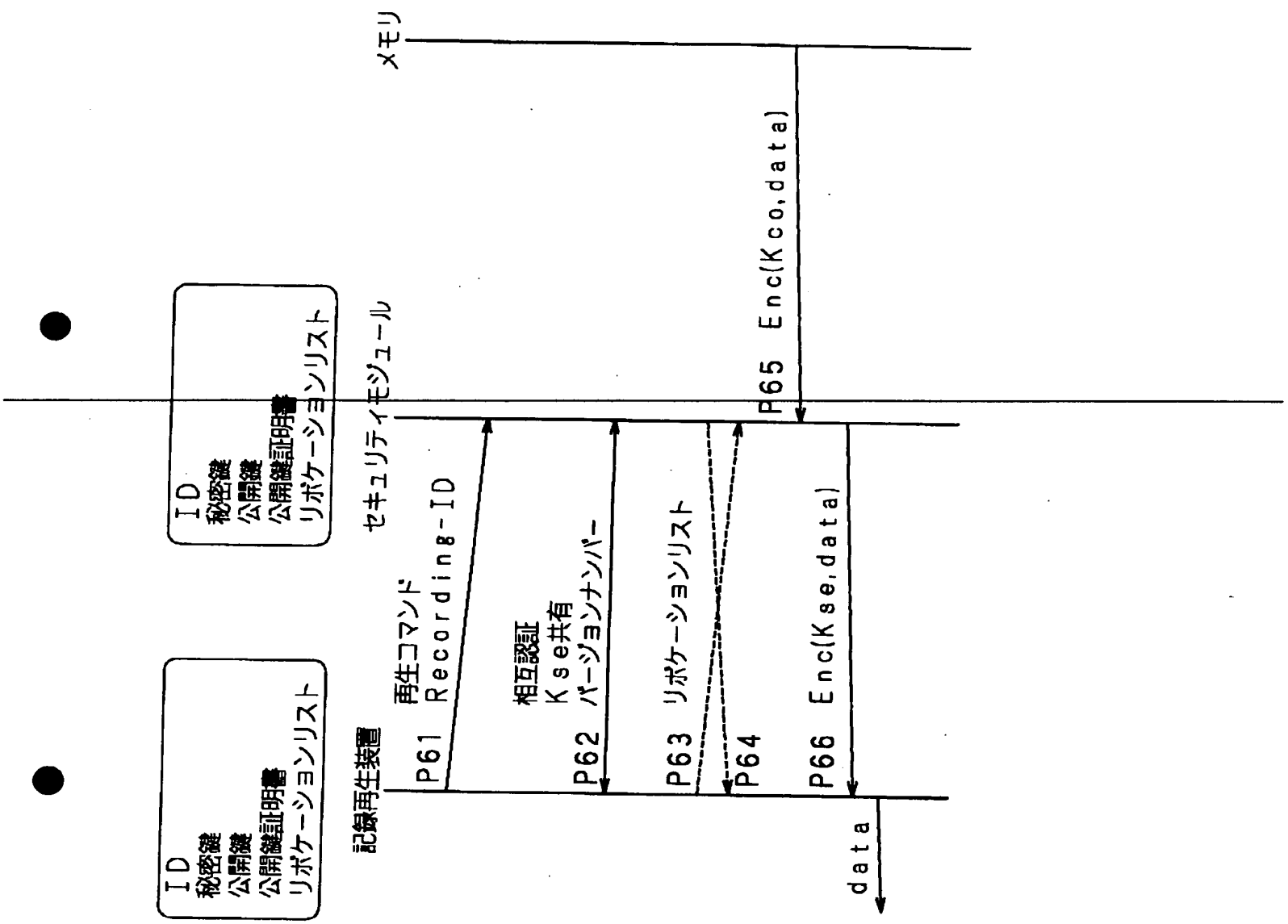
【図２０】


メモリ
セキュリティモジュール[A]
記録再生装置[B]
P41 再生コマンド,RB
VA=KAG
CertA,RA,RB,VA,RevVA,SigA
P42
CertA check
SigA check
IDA check
VB=KBG
CertB,RB,RA,VB,RevVB,SigB
P43
Kse=[KBVA]Isb_z
P44 リボケーションリスト
P45
RevVA check
TCsig check
CertB check
SigB check
IDB check
Kse=[KAVB]Isb_z
RevVB check
TCsig check
P46 Enc(Kst,Kco)
P47 Enc(Kst,Kco)
P48 Enc(Kco,data)
P49 Enc(Kco,data)
data

【図２１】


メモリ
セキュリティモジュール[A]
記録再生装置[B]
P51 再生コマンド,RB
VA=KAG
CertA,RA,RB,VA,RevVA,SigA
P52
CertB,RB,RA,VB,RevVB,SigB
P53
CertB check
SigBcheck,RevVB check
Kse=[KAVB]Isb_z
IDB check
IDB check
リボケーションリスト
P54
RevVB check
IDB check
TCsig check
リボケーションリスト
P55
P56 Enc(Kst,Kco)
P57 Enc(Kst,Kco)
P58 Enc(Kco,data)
P59 Enc(Kco,data)
data
Kse=[KBVA]Isb_z
バージョンが同じ場合
IDA check
モジュールのリストが新しい場合
RevVA check
IDA check
TCsig check
機器のリストが新しい場合
IDA check
CertA check
SigA check
VB=KBG
RevVA check

【図２２】

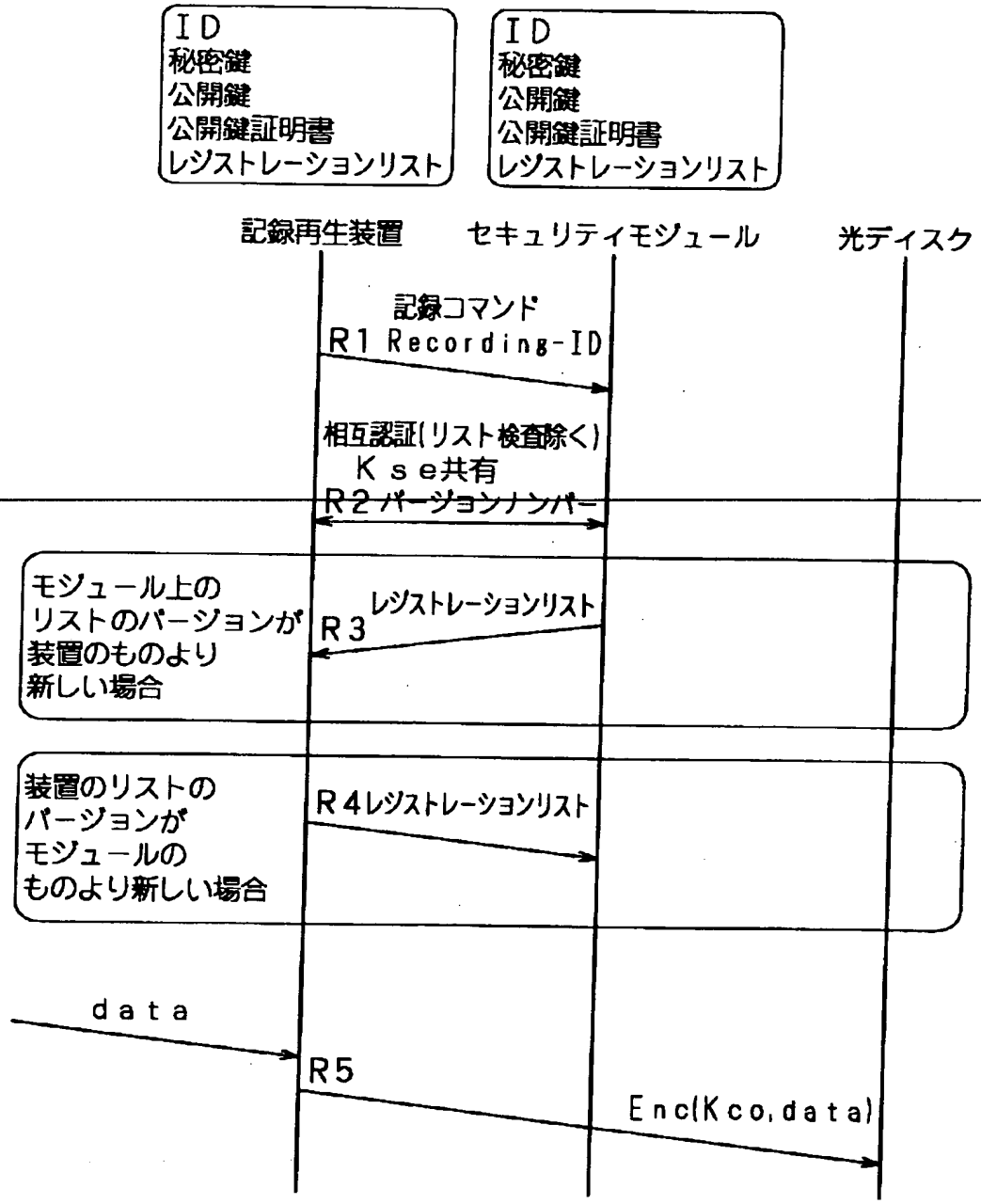

メモリ
ID
秘密鍵
公開鍵
公開鍵証明書
リボケーションリスト
セキュリティモジュール
P65 Enc(Kco,data)
ID
秘密鍵
公開鍵
公開鍵証明書
リボケーションリスト
記録再生装置
再生コマンド
Recording-ID
P61
相互認証
Kse共有
バージョンナンバー
P62
リボケーションリスト
P63
P64
P66 Enc(Kse,data)
data

【図２３】

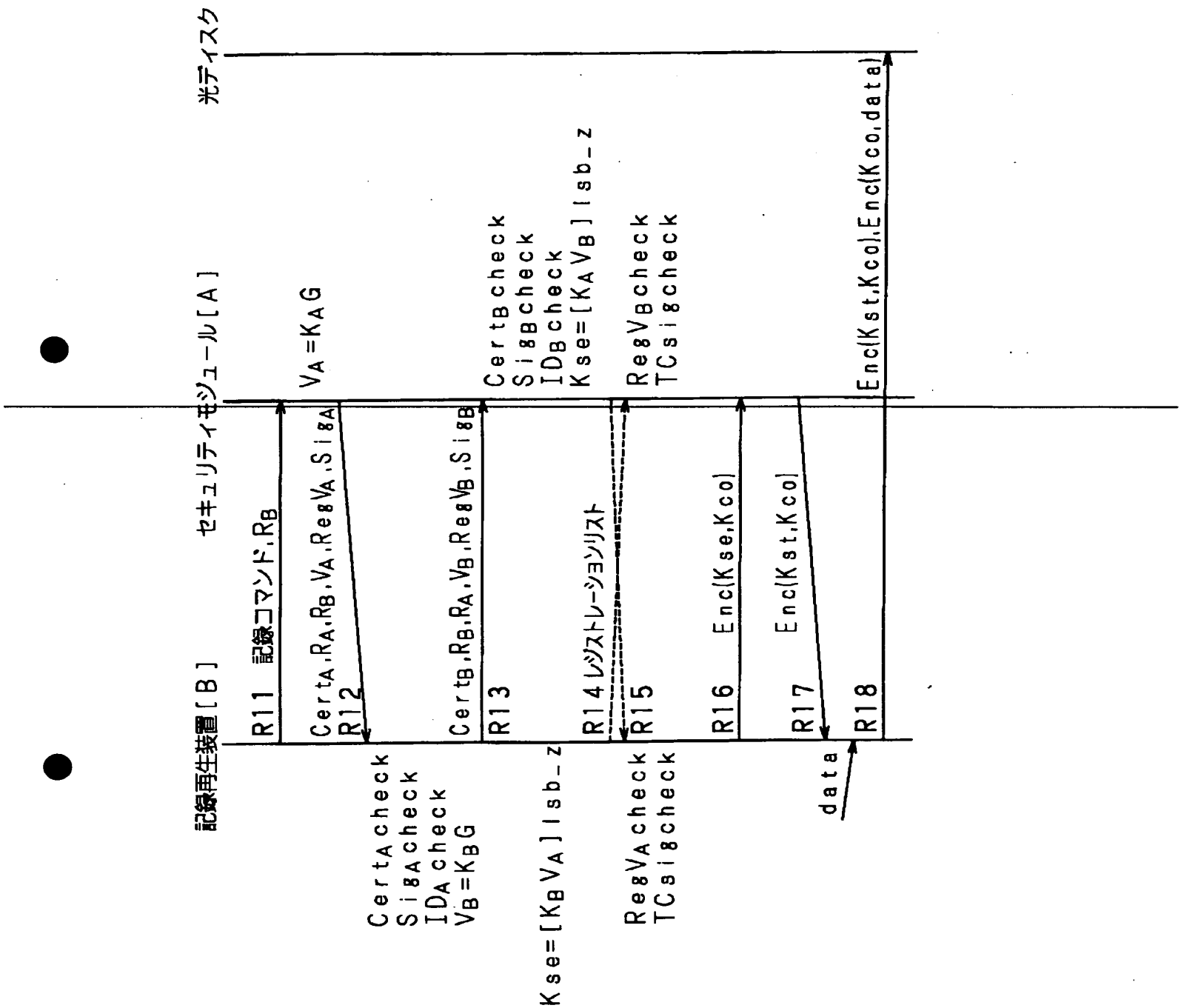
レジストレーションリスト

バージョンナンバー
登録される機器または媒体のＩＤ
・・・・・・
ＴＣのデジタル署名

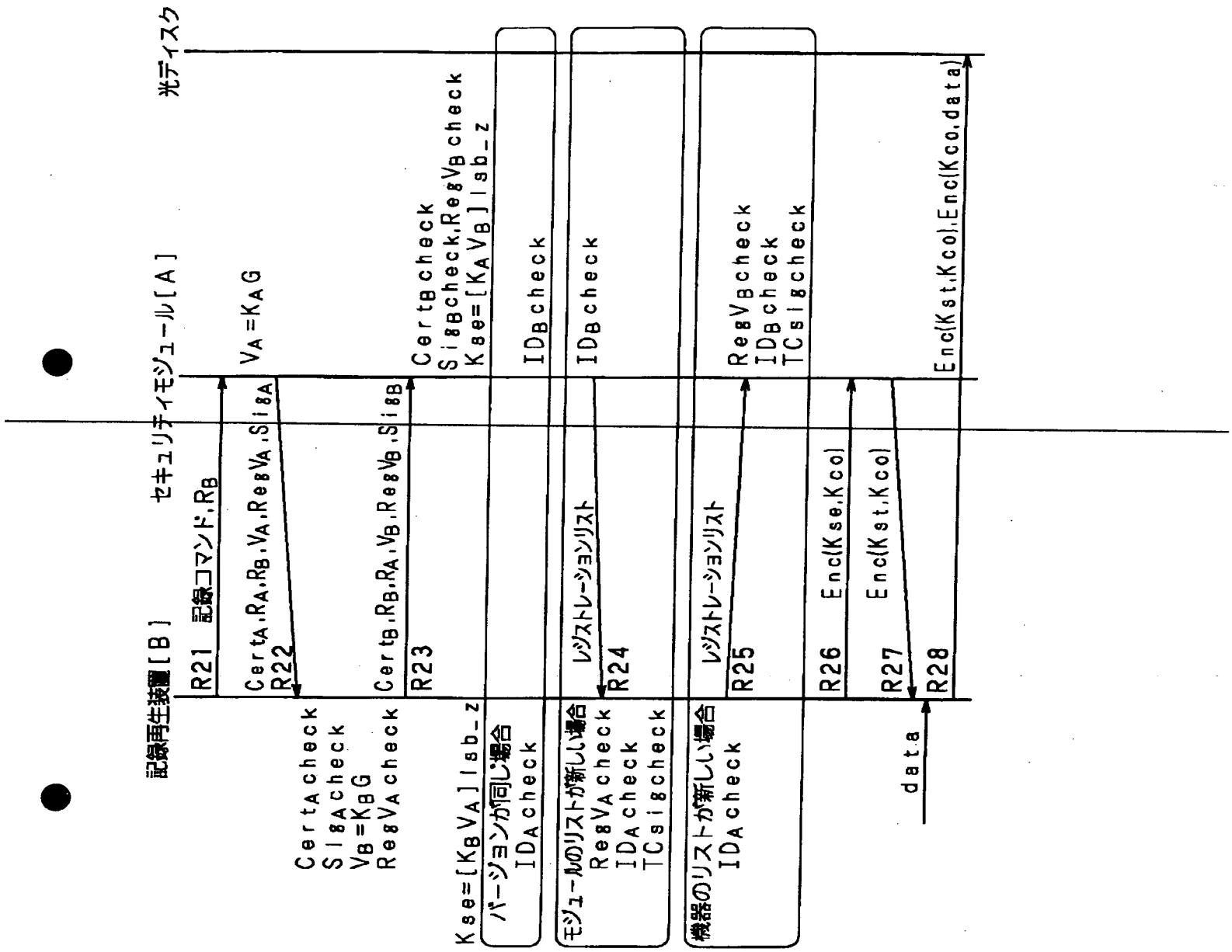
【図２４】


ＩＤ
秘密鍵
公開鍵
公開鍵証明書
レジストレーションリスト
ＩＤ
秘密鍵
公開鍵
公開鍵証明書
レジストレーションリスト
記録再生装置
セキュリティモジュール
光ディスク
記録コマンド
R1 Recording-ID
相互認証(リスト検査除く)
Ｋｓｅ共有
R2 バージョンナンバー
モジュール上の
リストのバージョンが
装置のものより
新しい場合
レジストレーションリスト
R3
装置のリストの
バージョンが
モジュールの
ものより新しい場合
R4レジストレーションリスト
ｄａｔａ
R5
Enc(Kco,data)

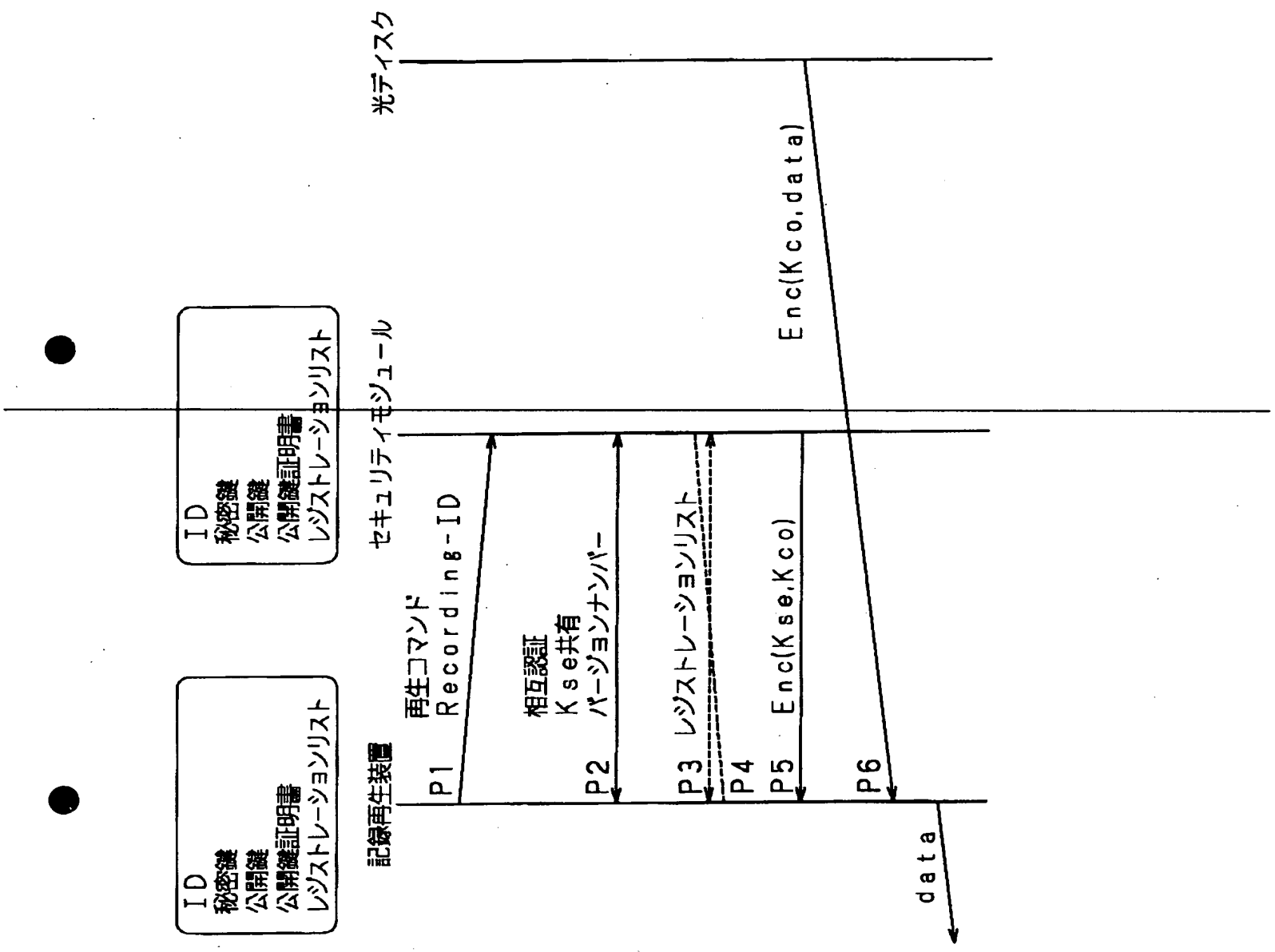
【図２５】


記録再生装置[B]
セキュリティモジュール[A]
光ディスク
R11 記録コマンド,RB
R12
CertA,RA,RB,VA,RegVA,SigA
VA=KAG
CertA check
SigA check
IDA check
VB=KBG
R13
CertB,RB,RA,VB,RegVB,SigB
CertB check
SigB check
IDB check
Kse=[KAVB]lsb_z
R14 レジストレーションリスト
R15
Kse=[KBVA]lsb_z
RegVB check
TCsig check
R16 Enc(Kse,Kco)
R17 Enc(Kst,Kco)
R18
Enc(Kst,Kco),Enc(Kco,data)
RegVA check
TCsig check
data

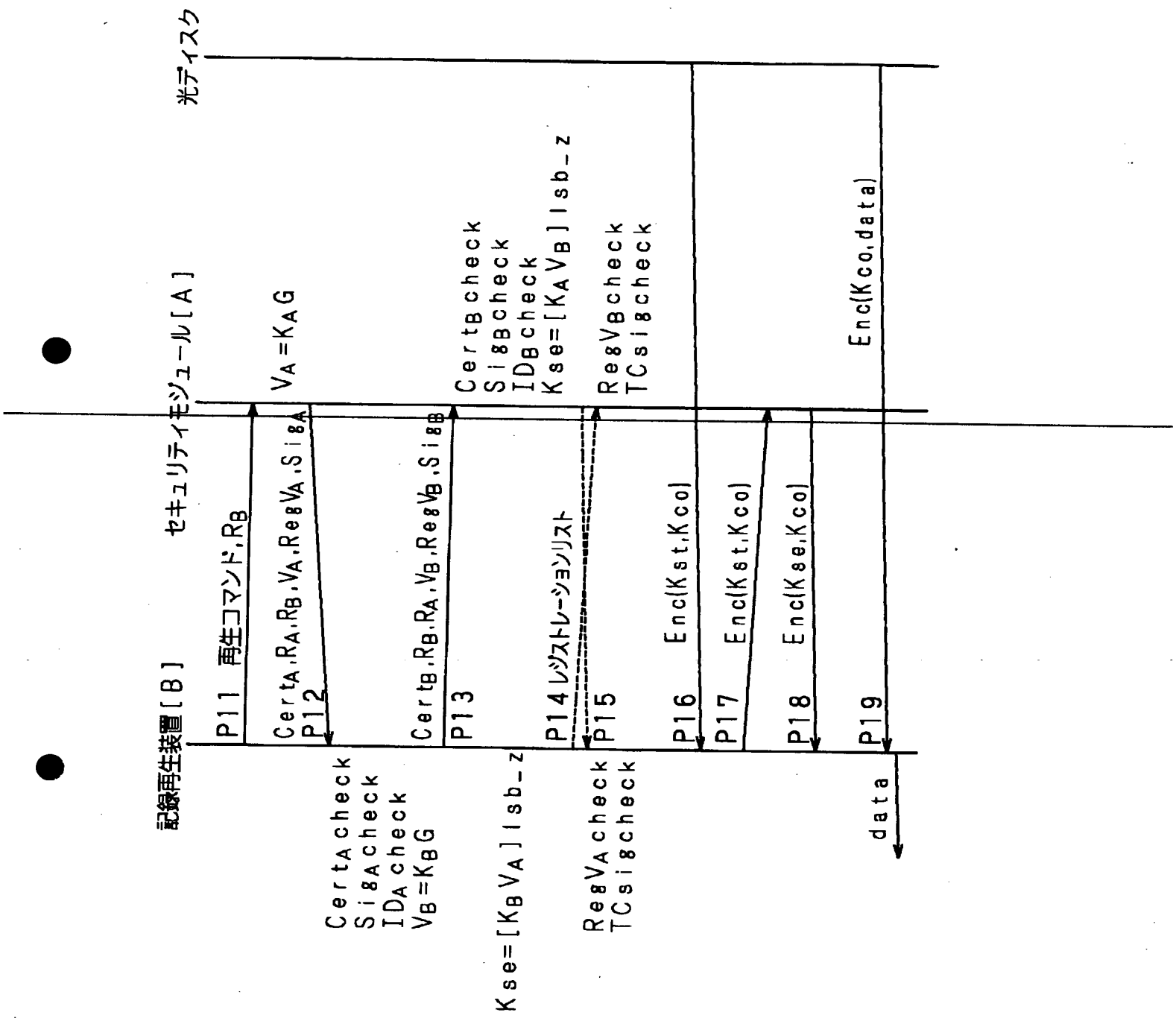
【図２６】


記録再生装置[B]
セキュリティモジュール[A]
光ディスク
R21 記録コマンド,RB
CertA,RA,RB,VA,RegVA,SigA
R22
VA=KAG
CertB,RB,RA,VB,RegVB,SigB
R23
CertB check
SigBcheck,RegVB check
Kse=[KAVB]Isb_z
IDB check
Kse=[KBVA]Isb_z
バージョンが同じ場合
IDA check
CertA check
SigA check
VB=KBG
RegVA check
モジュールのリストが新しい場合
RegVA check
IDA check
TCsig check
レジストレーションリスト
R24
機器のリストが新しい場合
IDA check
レジストレーションリスト
R25
RegVB check
IDB check
TCsig check
R26 Enc(Kse,Kcol)
R27 Enc(Kst,Kcol)
R28 Enc(Kst,Kcol),Enc(Kco,data)
data

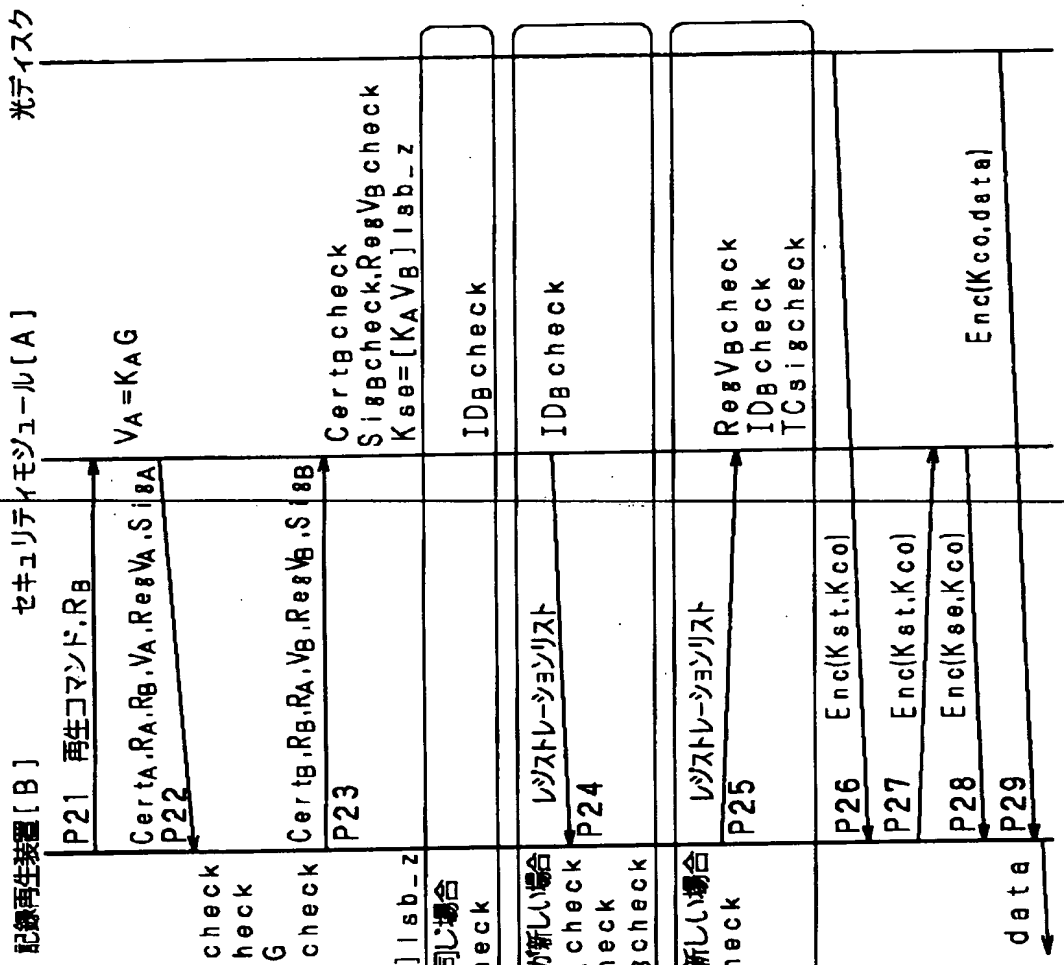
【図２７】


光ディスク
ID
秘密鍵
公開鍵
公開鍵証明書
レジストレーションリスト
セキュリティモジュール
Enc(Kco,data)
再生コマンド
Recording-ID
P1
相互認証
Kse共有
バージョンナンバー
P2
レジストレーションリスト
P3
P4
Enc(Kse,Kco)
P5
P6
記録再生装置
ID
秘密鍵
公開鍵
公開鍵証明書
レジストレーションリスト
data

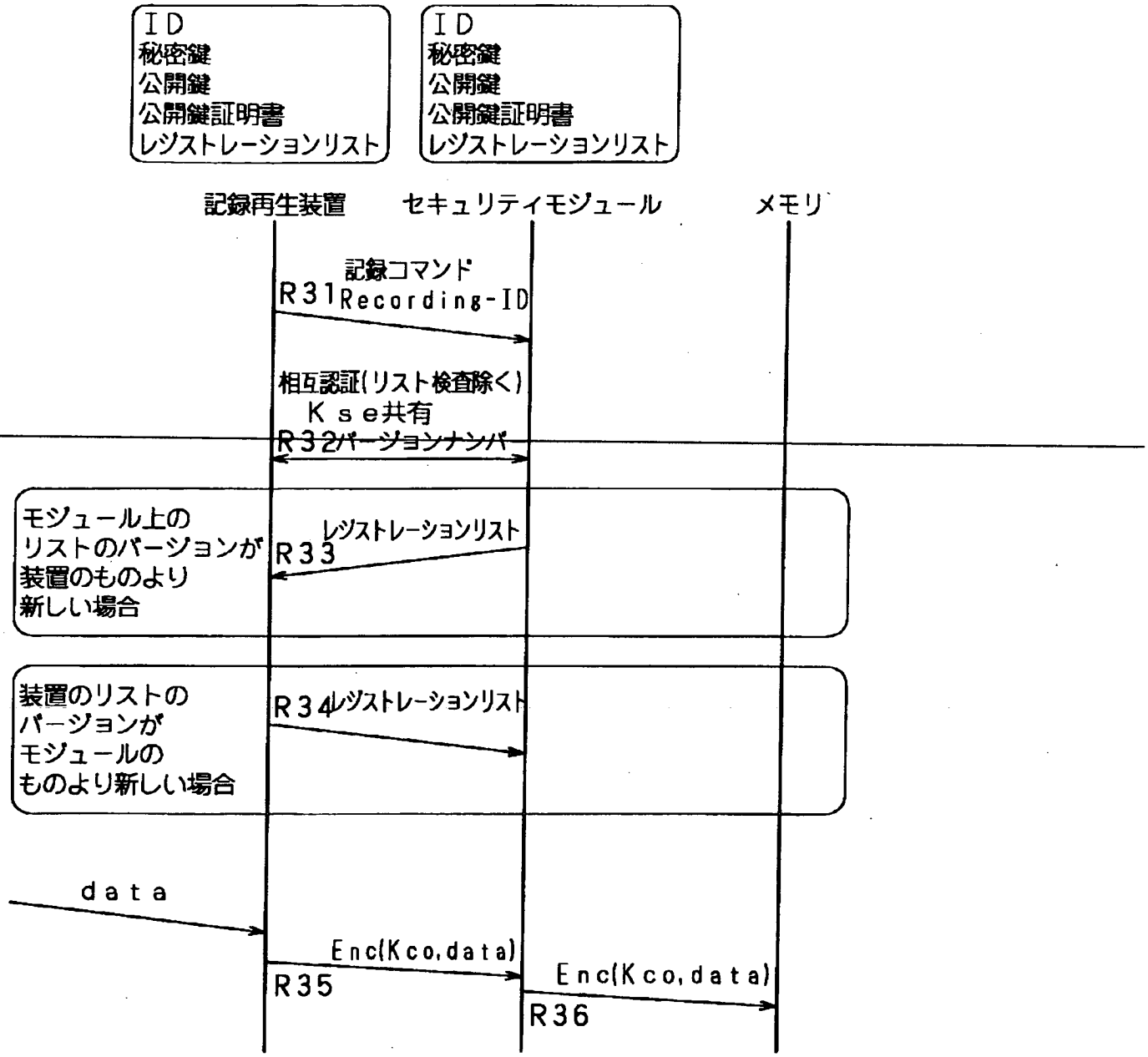
【図２８】


光ディスク
セキュリティモジュール[A]
記録再生装置[B]
P11 再生コマンド,RB
VA=KAG
CertA,RA,RB,VA,RegVA,SigA
P12
CertA check
SigA check
IDA check
VB=KBG
CertB,RB,RA,VB,RegVB,SigB
P13
CertB check
SigB check
IDB check
Kse=[KAVB]lsb_z
P14 リストレーションリスト
Kse=[KBVA]lsb_z
P15
RegVB check
TCsig check
RegVA check
TCsig check
P16 Enc(Kst,Kcol)
P17 Enc(Kst,Kcol)
P18 Enc(Kse,Kcol)
P19 Enc(Kco,data)
data

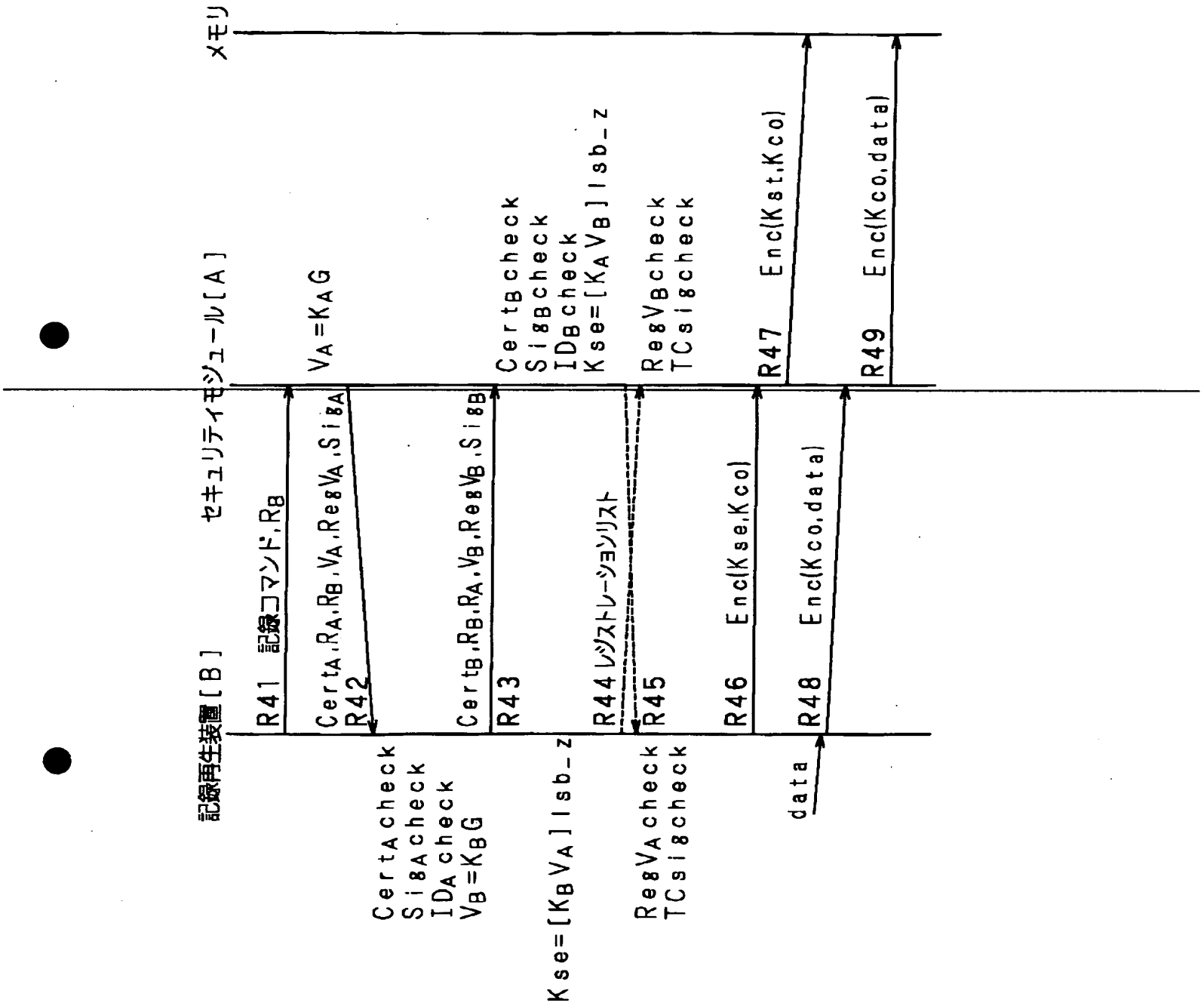
【図２９】


記録再生装置[B]
セキュリティモジュール[A]
光ディスク
P21 再生コマンド,RB
VA=KAG
CertA,RA,RB,VA,RegVA,SigA
P22
CertB,RB,RA,VB,RegVB,SigB
P23
CertB check
SigB check,RegVB check
Kse=[KAVB]Isb_z
IDB check
CertA check
SigA check
VB=KBG
RegVA check
Kse=[KBVA]Isb_z
バージョンが同じ場合
IDA check
レジストレーションリスト
P24
IDB check
モジュールのリストが新しい場合
RegVA check
IDA check
TCsig check
レジストレーションリスト
P25
RegVB check
IDB check
TCsig check
機器のリストが新しい場合
IDA check
Enc(Kst,Kco)
P26
Enc(Kst,Kco)
P27
Enc(Kse,Kco)
P28
Enc(Kco,data)
P29
data

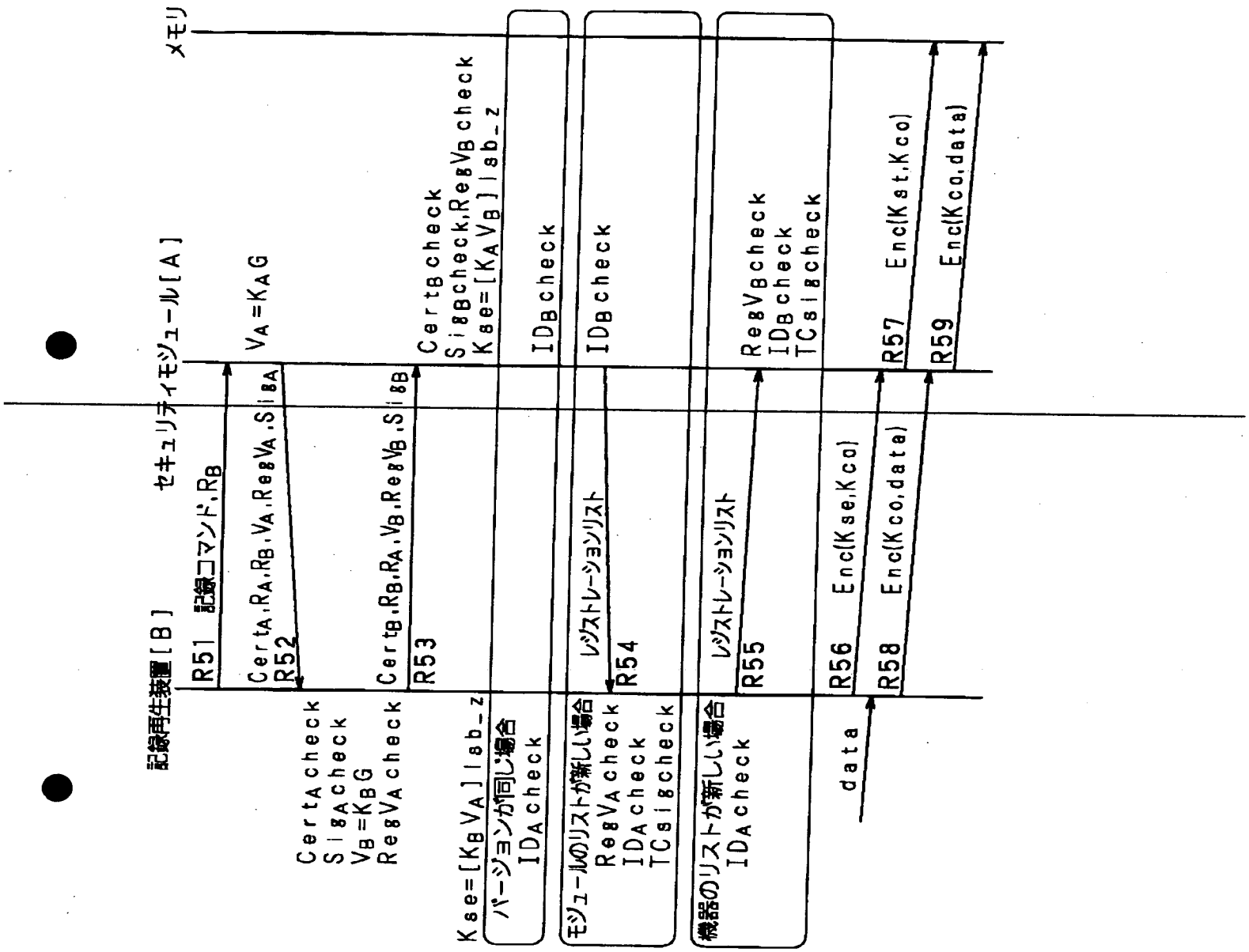
【図３０】


ＩＤ
秘密鍵
公開鍵
公開鍵証明書
レジストレーションリスト
ＩＤ
秘密鍵
公開鍵
公開鍵証明書
レジストレーションリスト
記録再生装置
セキュリティモジュール
メモリ
記録コマンド
R31 Recording-ID
相互認証(リスト検査除く)
Ｋｓｅ共有
R32 バージョンナンバ
モジュール上の
リストのバージョンが
装置のものより
新しい場合
レジストレーションリスト
R33
装置のリストの
バージョンが
モジュールの
ものより新しい場合
R34 レジストレーションリスト
ｄａｔａ
Enc(Kco,data)
R35
Enc(Kco,data)
R36

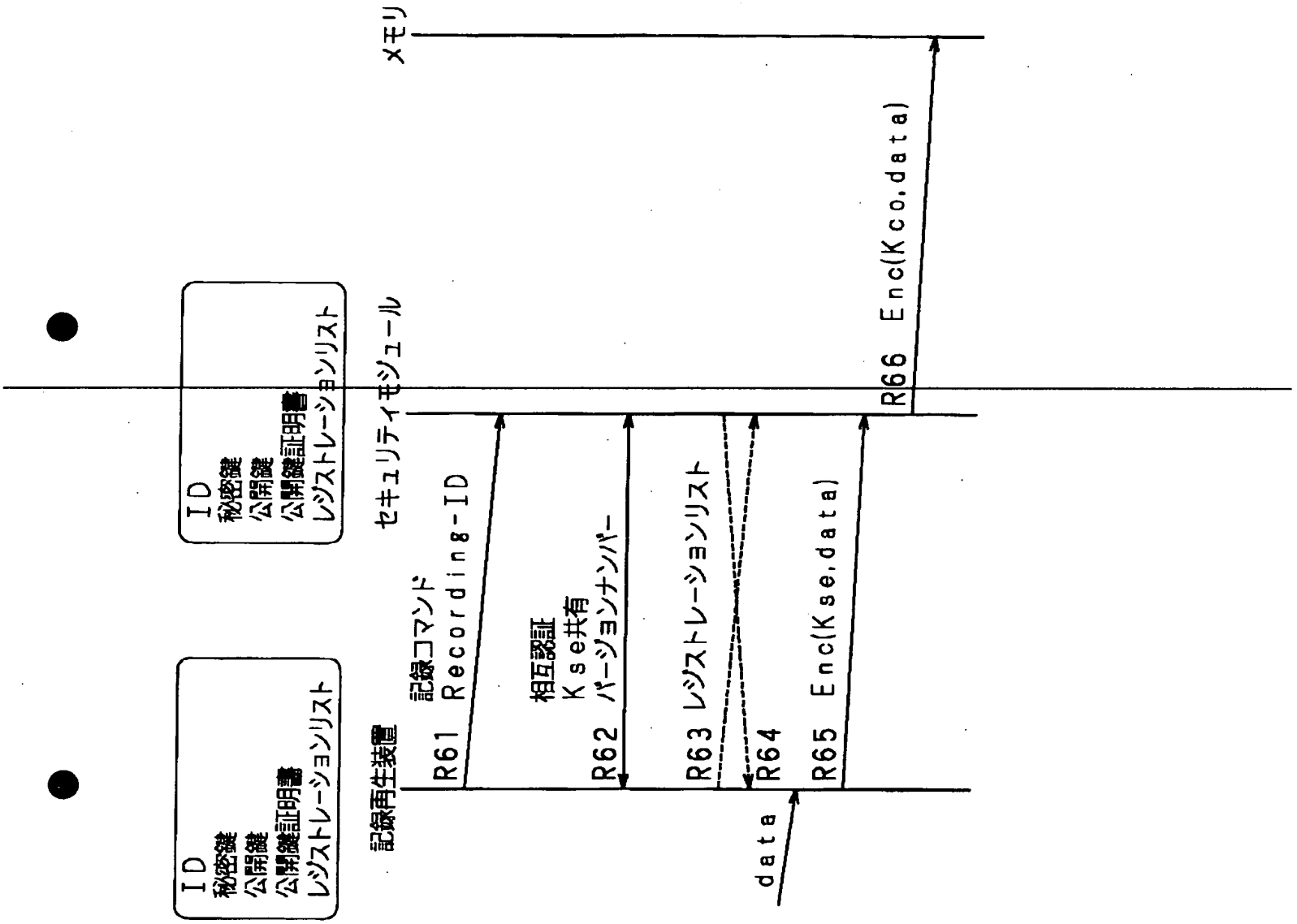
【図３１】


メモリ
セキュリティモジュール[A]
記録再生装置[B]
VA=KAG
CertBcheck
SigBcheck
IDBcheck
Kse=[KAVB]lsb_z
RegVBcheck
TCsigcheck
R47 Enc(Kst,Kcol)
R49 Enc(Kco,data)
R41 記録コマンド,RB
CertA,RA,RB,VA,RegVA,SigA
R42
CertB,RB,RA,VB,RegVB,SigB
R43
R44 レジストレーションリスト
R45
R46 Enc(Kse,Kcol)
R48 Enc(Kco,data)
CertAcheck
SigAcheck
IDAcheck
VB=KBG
Kse=[KBVA]lsb_z
RegVAcheck
TCsigcheck
data

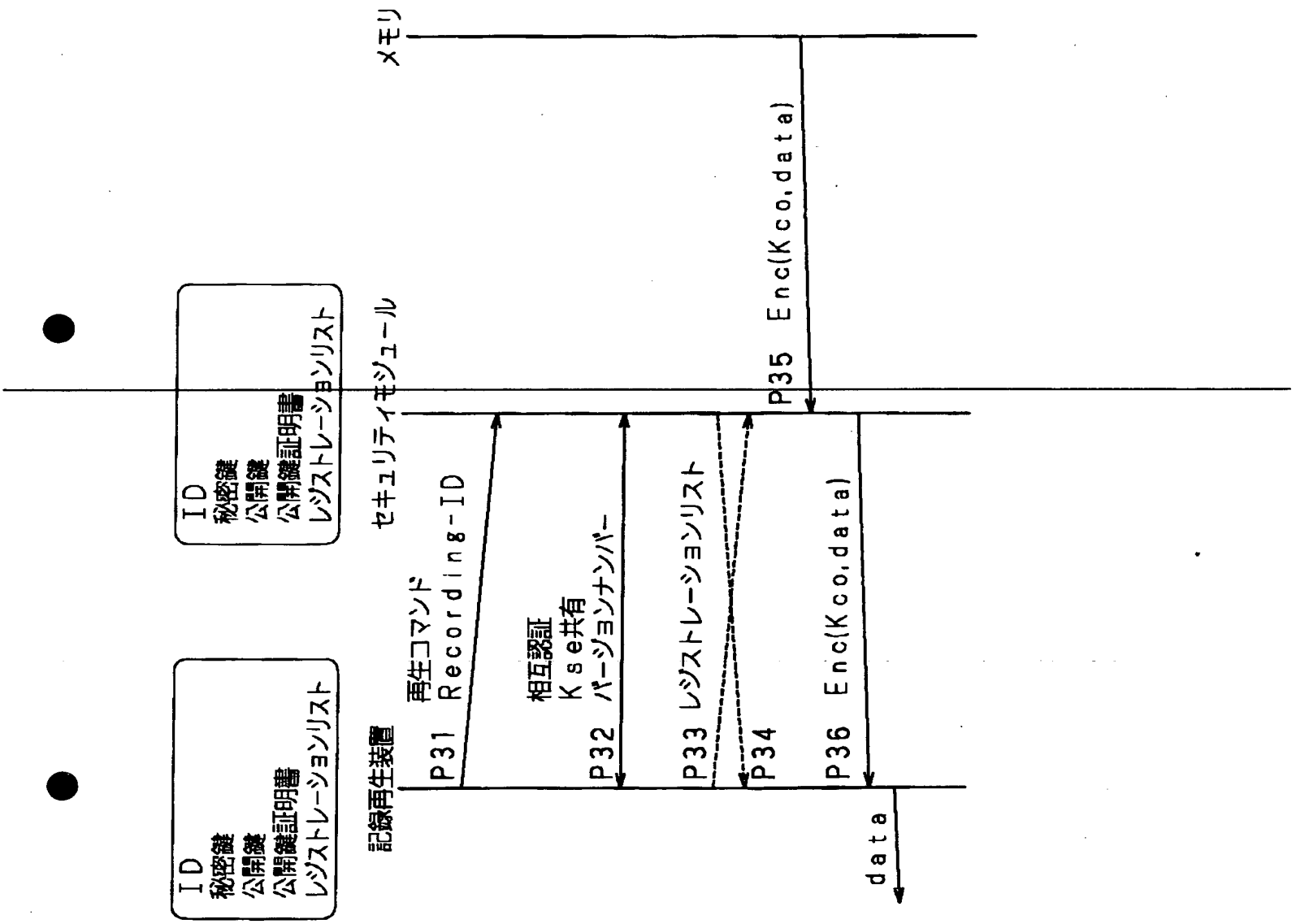
【図３２】


記録再生装置[B]
セキュリティモジュール[A]
メモリ
R51 記録コマンド,RB
VA=KAG
CertA,RA,RB,VA,RegVA,SigA
R52
CertB,RB,RA,VB,RegVB,SigB
R53
CertBcheck
SigBcheck,RegVBcheck
Kse=[KAVB]Isb_z
IDBcheck
IDBcheck
RegVBcheck
IDBcheck
TCsigcheck
R54
R55
R56 Enc(Kse,Kco)
R57 Enc(Kst,Kco)
R58 Enc(Kco,data)
R59 Enc(Kco,data)
data
CertAcheck
SigAcheck
VB=KBG
RegVAcheck
Kse=[KBVA]Isb_z
バージョンが同じ場合
IDAcheck
モジュールのリストが新しい場合
RegVAcheck
IDAcheck
TCsigcheck
レジストレーションリスト
レジストレーションリスト
機器のリストが新しい場合
IDAcheck

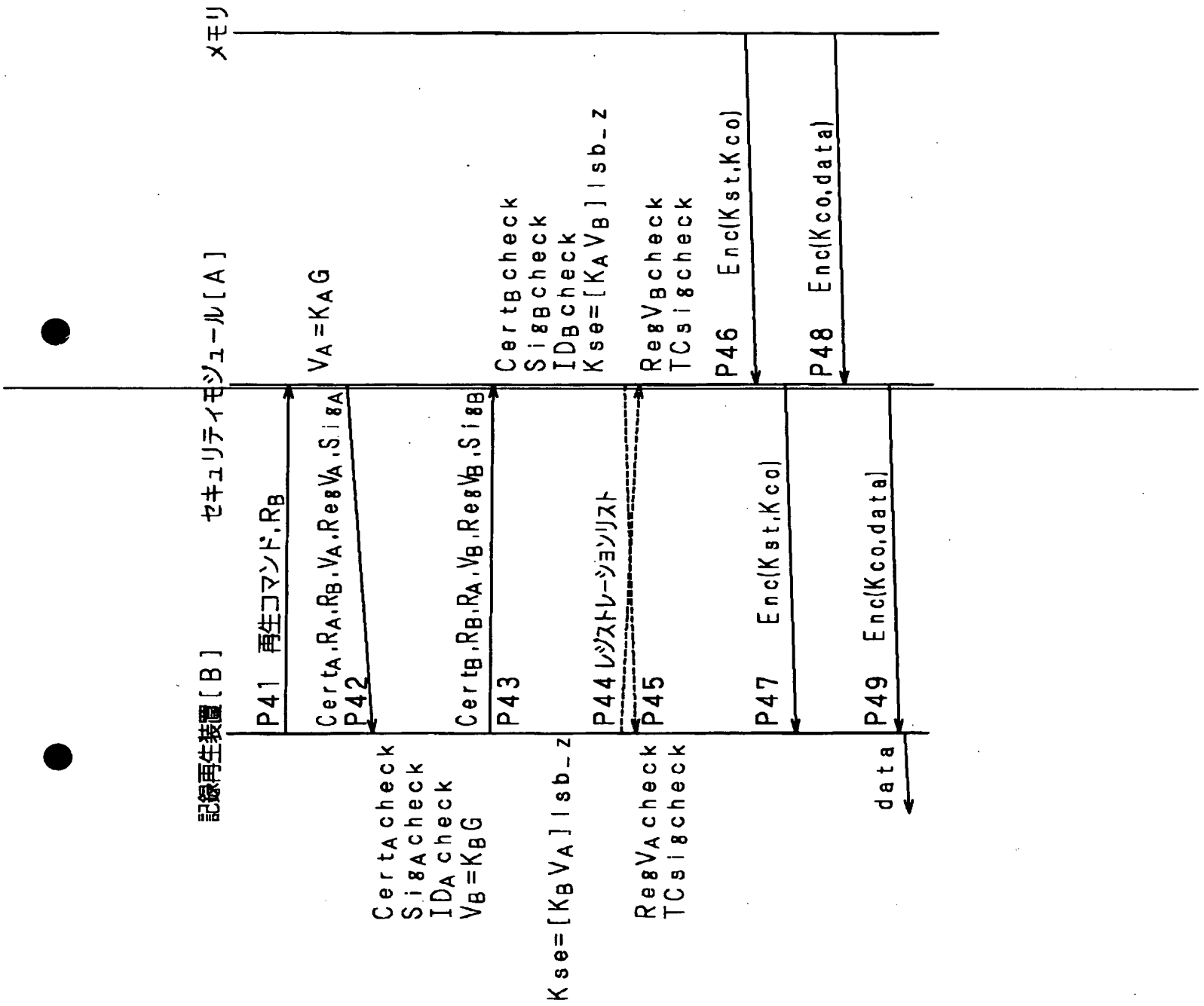
【図３３】


メモリ
ID
秘密鍵
公開鍵
公開鍵証明書
レジストレーションリスト
セキュリティモジュール
R66 Enc(Kco,data)
記録コマンド
R61 Recording-ID
相互認証
Kse共有
R62 バージョンナンバー
R63 レジストレーションリスト
R64
R65 Enc(Kse,data)
記録再生装置
ID
秘密鍵
公開鍵
公開鍵証明書
レジストレーションリスト
data

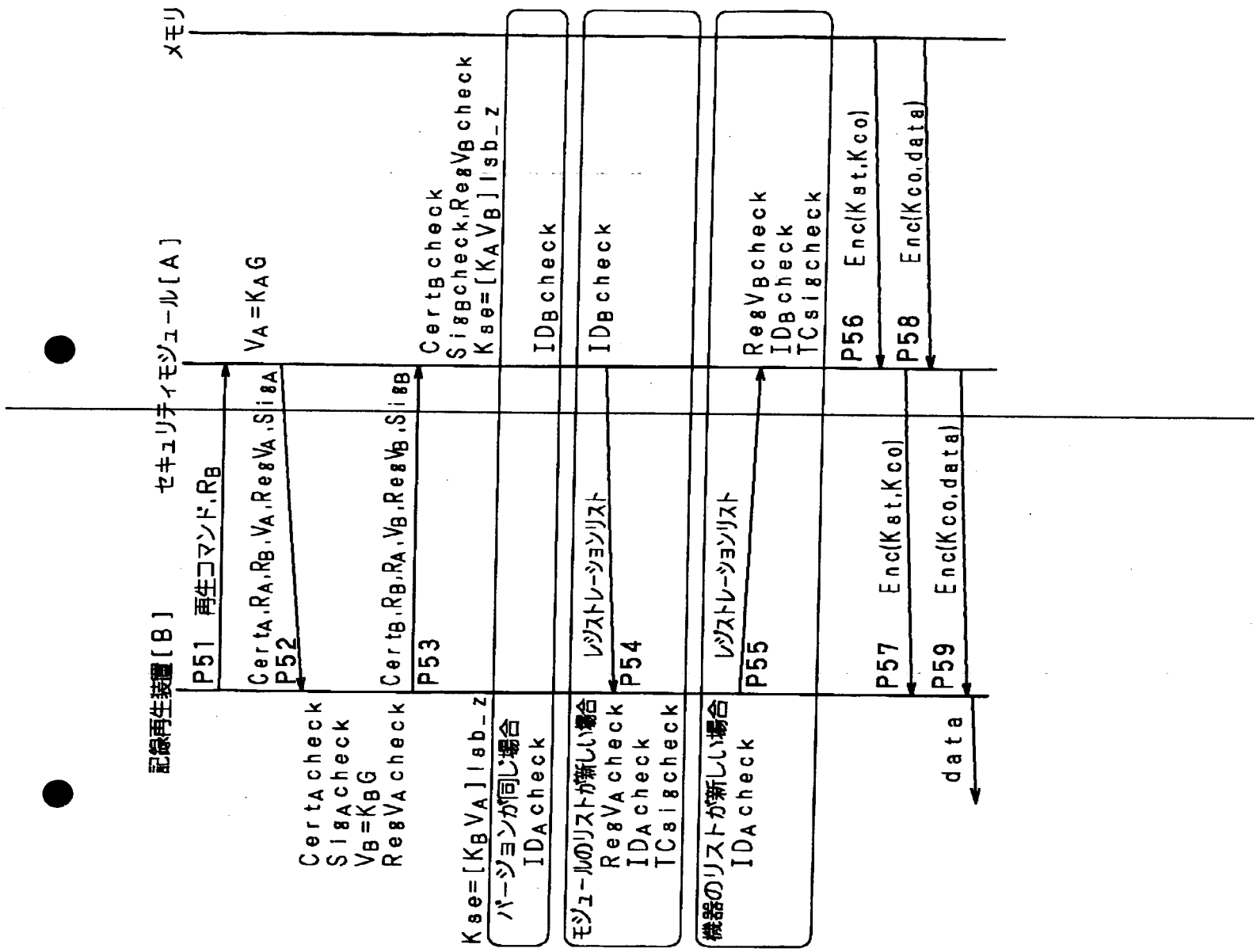
【図３４】


メモリ
セキュリティモジュール
記録再生装置
ID
秘密鍵
公開鍵
公開鍵証明書
レジストレーションリスト
ID
秘密鍵
公開鍵
公開鍵証明書
レジストレーションリスト
再生コマンド
Recording-ID
P31
相互認証
Kse共有
バージョンナンバー
P32
P33 レジストレーションリスト
P34
P35 Enc(Kco,data)
P36 Enc(Kco,data)
data

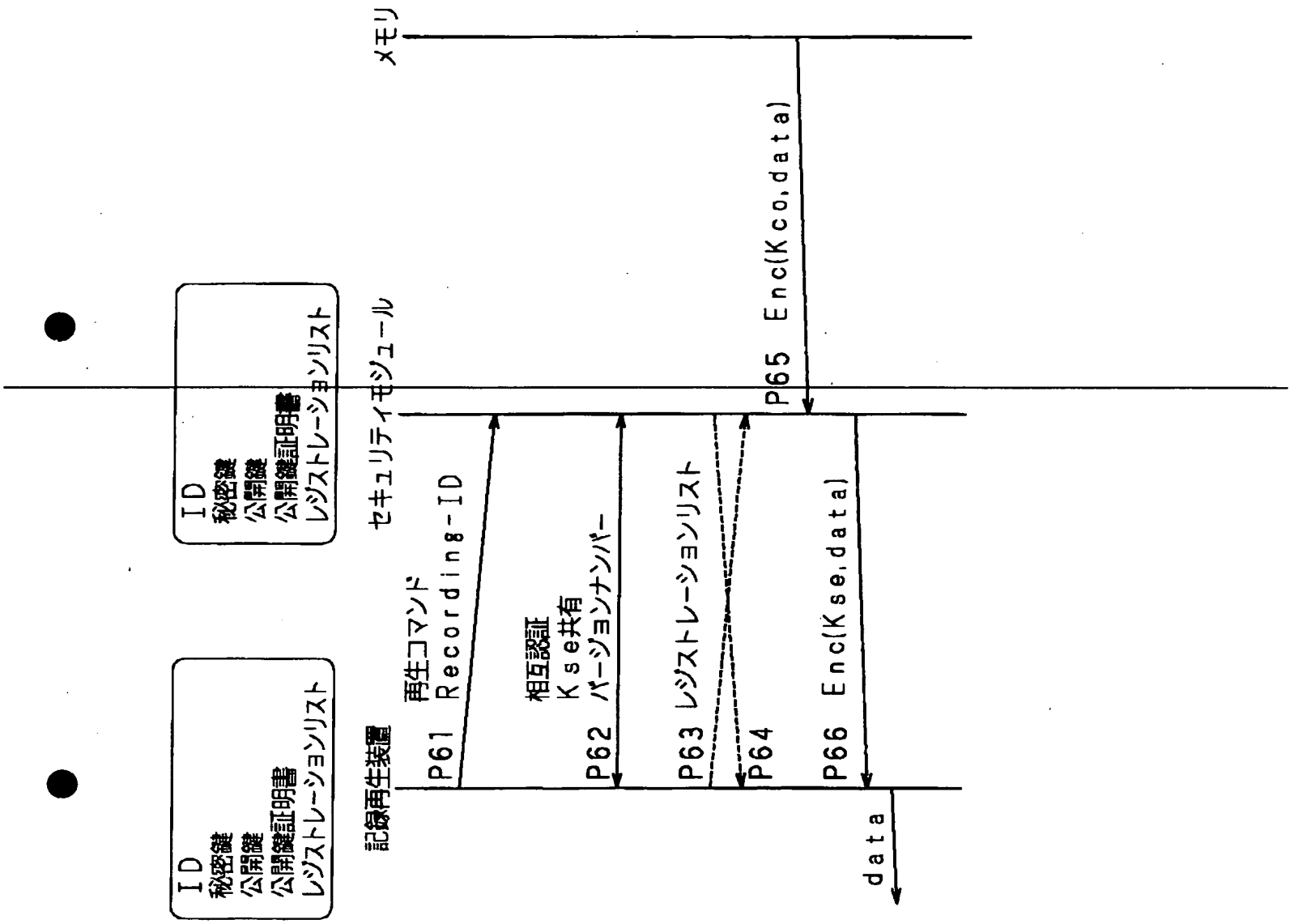
【図３５】


メモリ
セキュリティモジュール[A]
記録再生装置[B]
P41 再生コマンド,RB
VA=KAG
CertA,RA,RB,VA,RegVA,SigA
P42
CertA check
SigA check
IDA check
VB=KBG
CertB,RB,RA,VB,RegVB,SigB
P43
CertB check
SigB check
IDB check
Kse=[KAVB]lsb_z
P44 レジストレーションリスト
P45
RegVB check
TCsig check
P46 Enc(Kst,Kco)
P47 Enc(Kst,Kco)
P48 Enc(Kco,data)
P49 Enc(Kco,data)
Kse=[KBVA]lsb_z
RegVA check
TCsig check
data

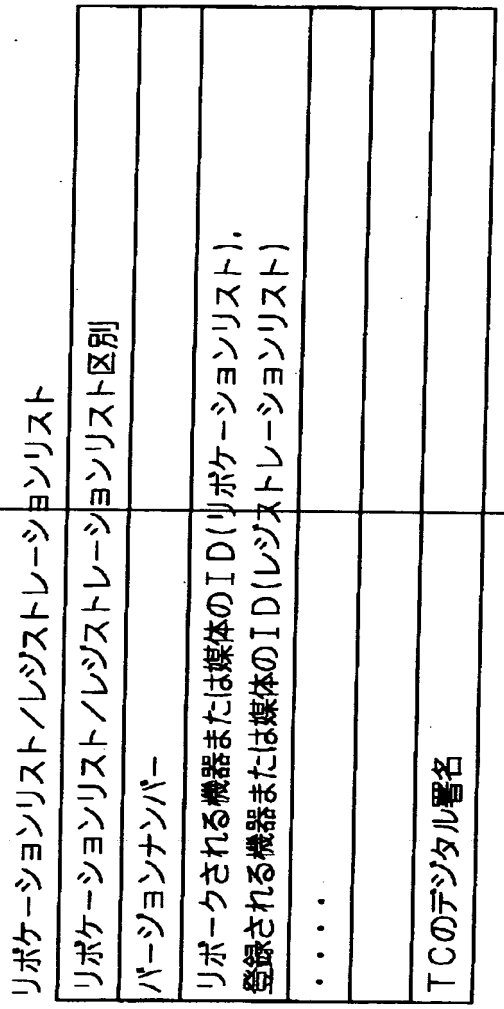
【図３６】


記録再生装置[B]
セキュリティモジュール[A]
メモリ
P51 再生コマンド,RB
CertA,RA,RB,VA,RegVA,SigA
P52
CertB,RB,RA,VB,RegVB,SigB
P53
P54
P55
P56 Enc(Kst,Kco)
P57 Enc(Kst,Kco)
P58 Enc(Kco,data)
P59 Enc(Kco,data)
data
VA=KAG
CertB check
SigBcheck,RegVB check
Kse=[KAVB]lsb_z
IDB check
IDB check
RegVB check
IDB check
TCsig check
CertA check
SigA check
VB=KBG
RegVA check
Kse=[KBVA]lsb_z
バージョンが同じ場合
IDA check
モジュールのリストが新しい場合
RegVA check
IDA check
TCsig check
機器のリストが新しい場合
IDA check

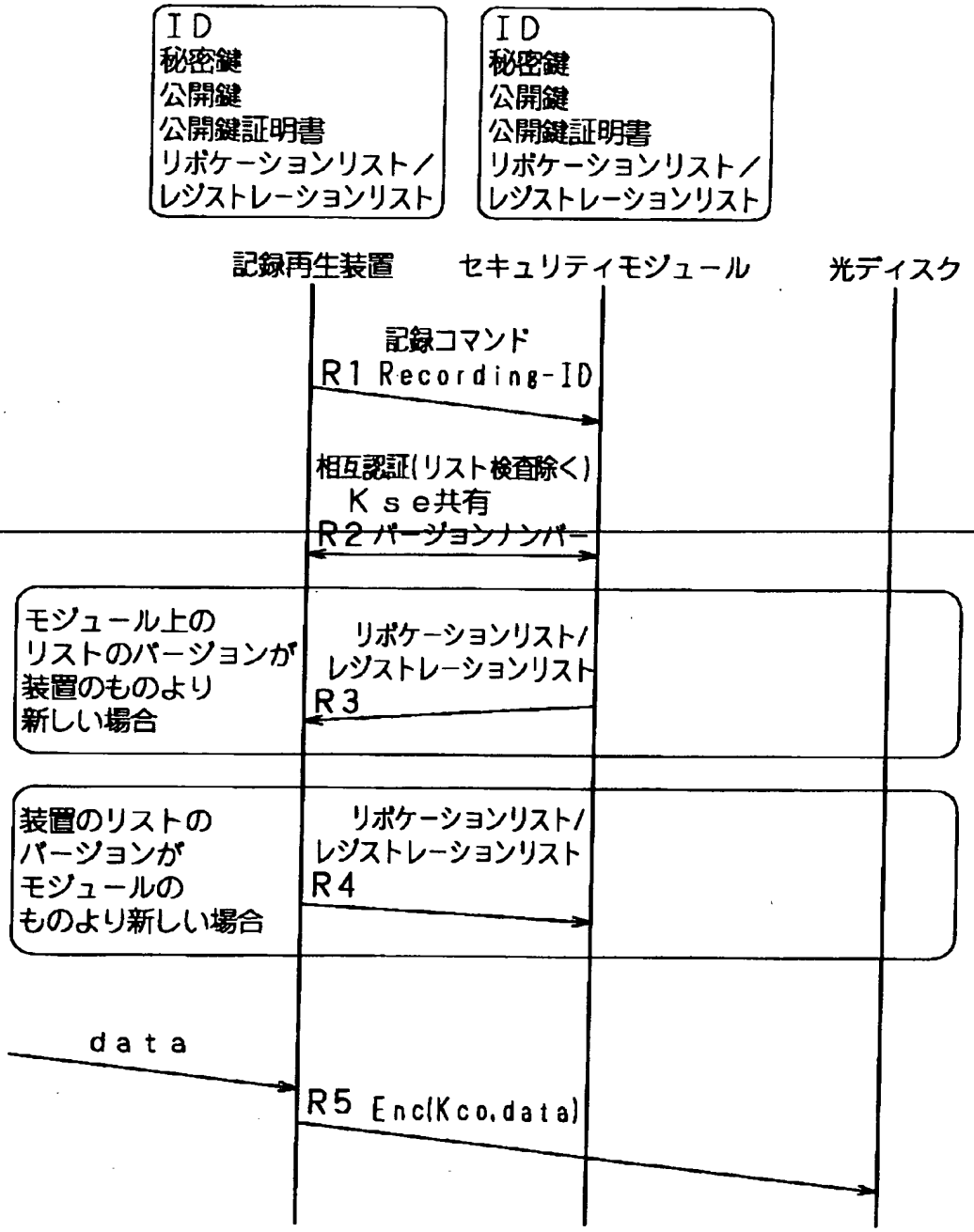
【図３７】


メモリ
セキュリティモジュール
記録再生装置
ID
秘密鍵
公開鍵
公開鍵証明書
レジストレーションリスト
ID
秘密鍵
公開鍵
公開鍵証明書
レジストレーションリスト
再生コマンド
P61 Recording-ID
相互認証
Kse共有
P62 バージョンナンバー
P63 レジストレーションリスト
P64
P65 Enc(Kco,data)
P66 Enc(Kse,data)
data

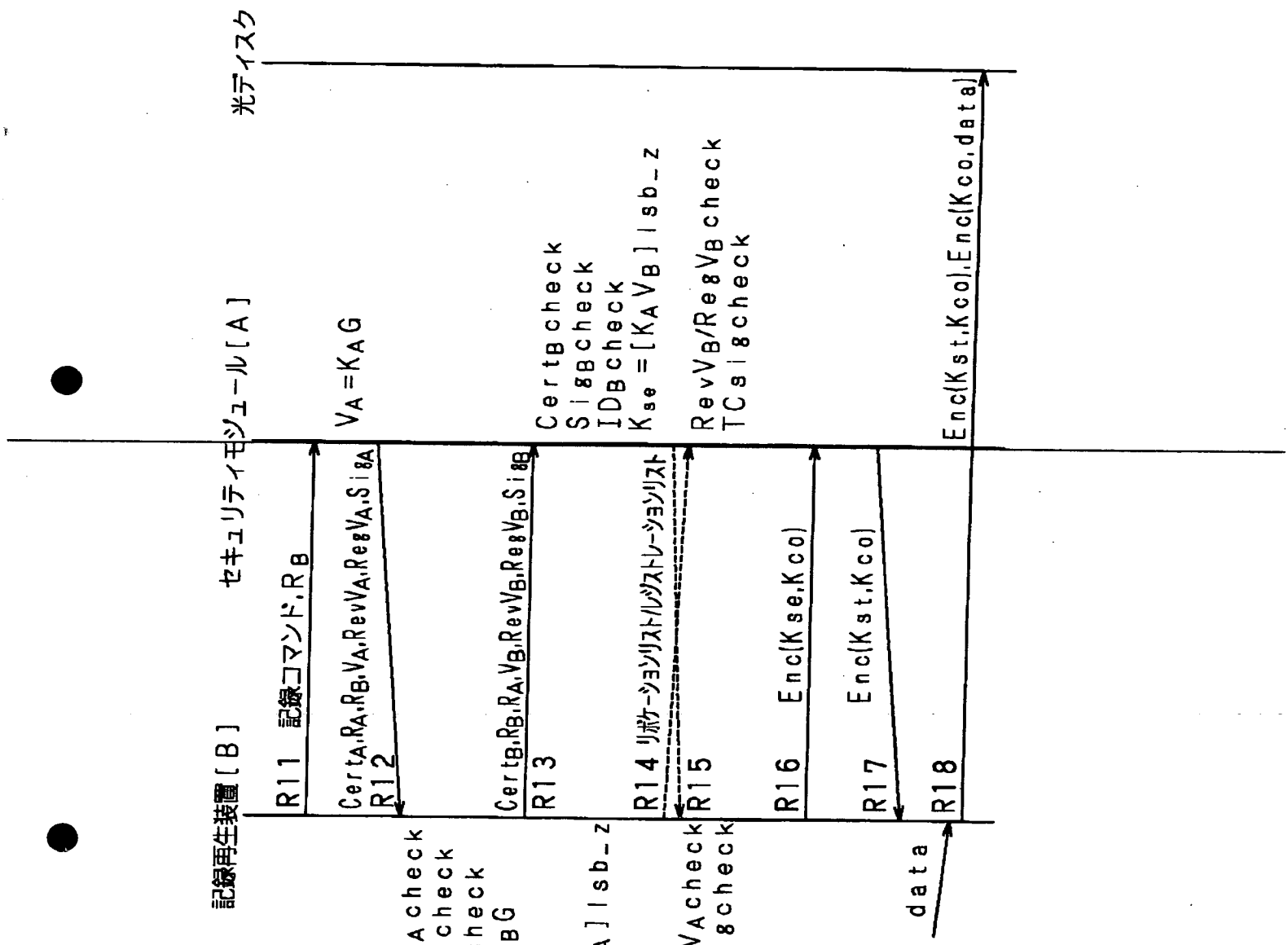
【図３８】


リポケーションリスト／レジストレーションリスト
リポケーションリスト／レジストレーションリスト区別
バージョンナンバー
リポークされる機器または媒体のＩＤ（リポケーションリスト），
登録される機器または媒体のＩＤ（レジストレーションリスト）
・・・・
ＴＣのデジタル署名

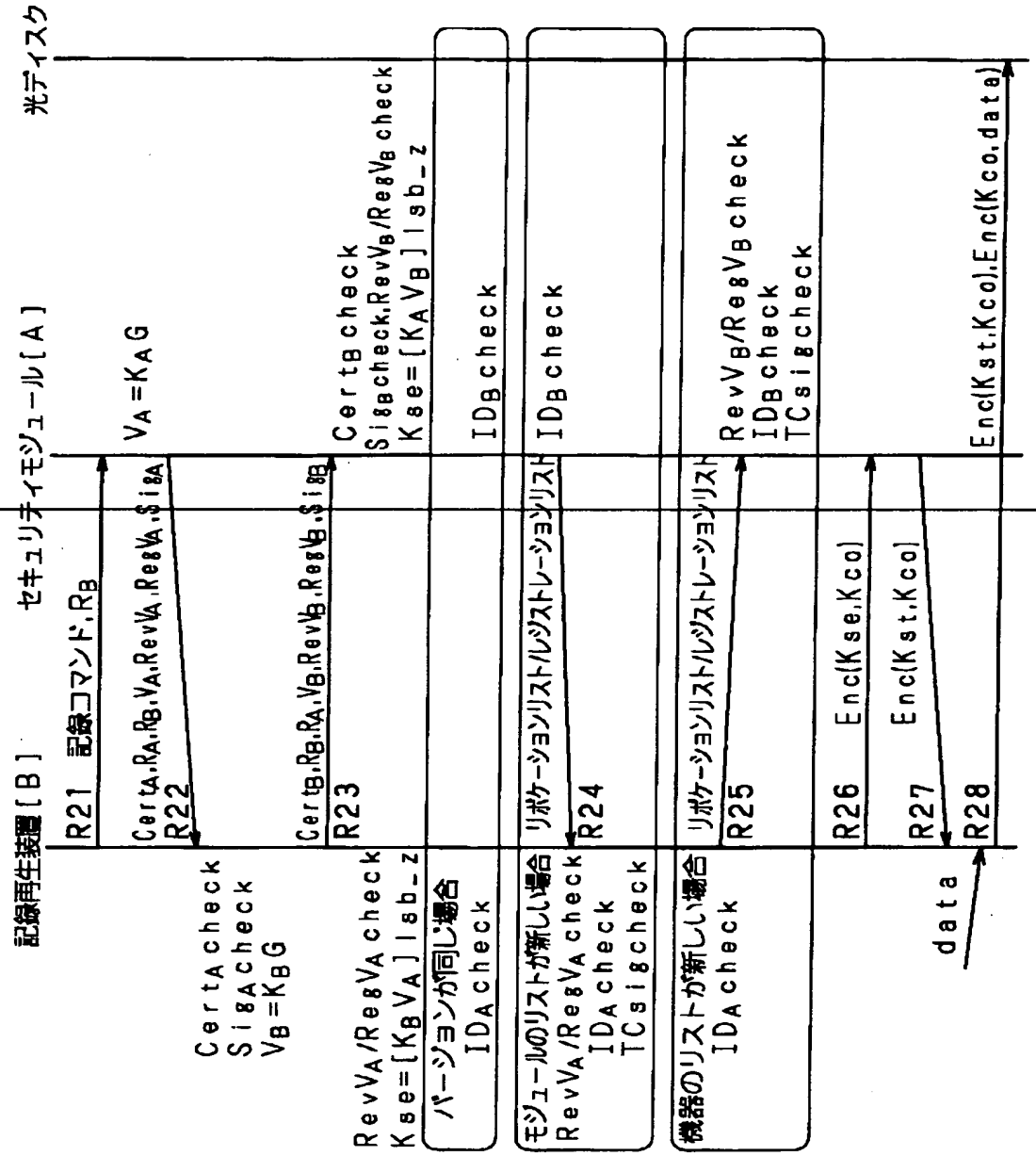
【図３９】


ＩＤ
秘密鍵
公開鍵
公開鍵証明書
リボケーションリスト／
レジストレーションリスト
ＩＤ
秘密鍵
公開鍵
公開鍵証明書
リボケーションリスト／
レジストレーションリスト
記録再生装置
セキュリティモジュール
光ディスク
記録コマンド
R1 Recording-ID
相互認証(リスト検査除く)
Ｋｓｅ共有
R2 バージョンナンバー
モジュール上の
リストのバージョンが
装置のものより
新しい場合
リボケーションリスト/
レジストレーションリスト
R3
装置のリストの
バージョンが
モジュールの
ものより新しい場合
リボケーションリスト/
レジストレーションリスト
R4
ｄａｔａ
R5 Enc(Kco,data)

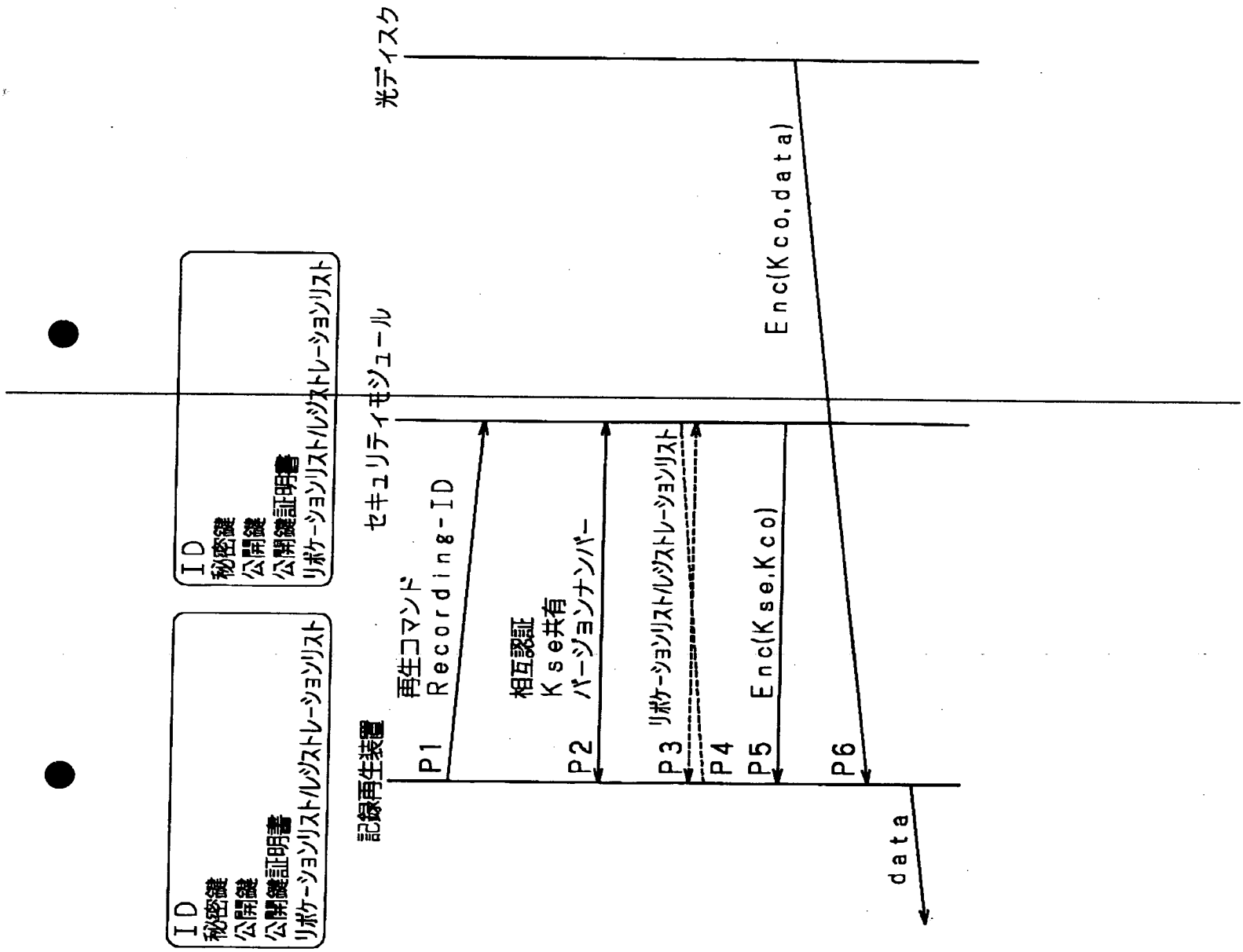
【図４０】


記録再生装置[B]
セキュリティモジュール[A]
光ディスク
R11 記録コマンド,RB
CertA,RA,RB,VA,RevVA,RegVA,SigA
R12
CertB,RB,RA,VB,RevVB,RegVB,SigB
R13
R14 リボケーションリストリジストレーションリスト
R15
R16 Enc(Kse,Kco)
R17 Enc(Kst,Kco)
R18
data
VA=KAG
CertA check
SigA check
IDA check
VB=KBG
Kse=[KBVA]lsb_z
CertB check
SigB check
IDB check
Kse=[KAVB]lsb_z
RevVA/RegVA check
TC sig check
RevVB/RegVB check
TC sig check
Enc(Kst,Kco),Enc(Kco,data)

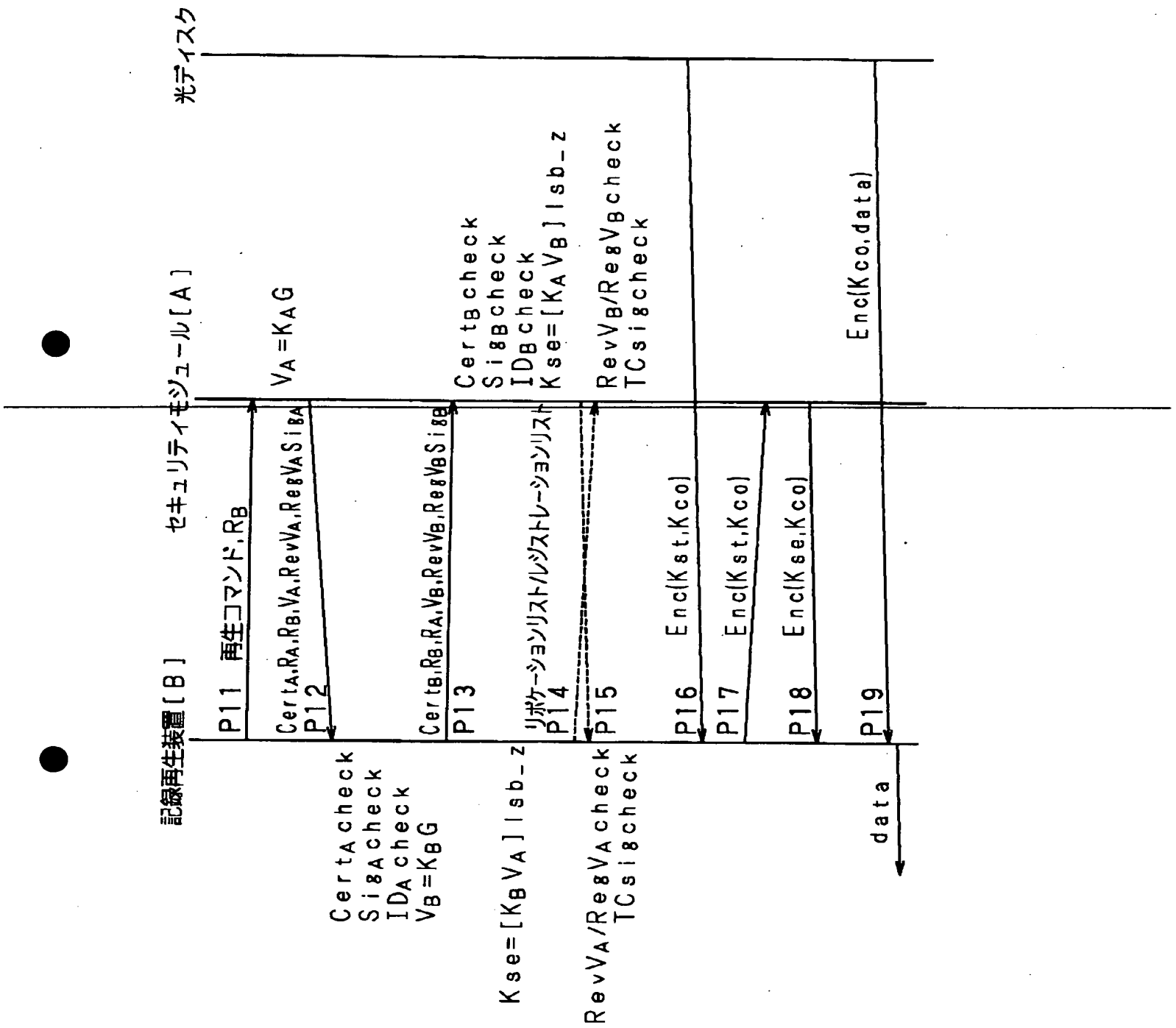
【図４１】


記録再生装置[B]
セキュリティモジュール[A]
光ディスク
R21 記録コマンド,RB
VA=KAG
CertA,RA,RB,VA,RevVA,RegVA,SigA
R22
CertB,RB,RA,VB,RevVB,RegVB,SigB
R23
CertB check
SigBcheck,RevVB/RegVB check
Kse=[KA VB]Isb_z
IDB check
CertA check
SigA check
VB=KBG
RevVA/RegVA check
Kse=[KB VA]Isb_z
バージョンが同じ場合
IDA check
リボケーションリスト/レジストレーションリスト
R24
モジュールのリストが新しい場合
RevVA/RegVA check
IDA check
TCsig check
リボケーションリスト/レジストレーションリスト
R25
機器のリストが新しい場合
IDA check
RevVB/RegVB check
IDB check
TCsig check
R26 Enc(Kse,Kco)
R27 Enc(Kst,Kco)
R28
Enc(Kst,Kco),Enc(Kco,data)
data

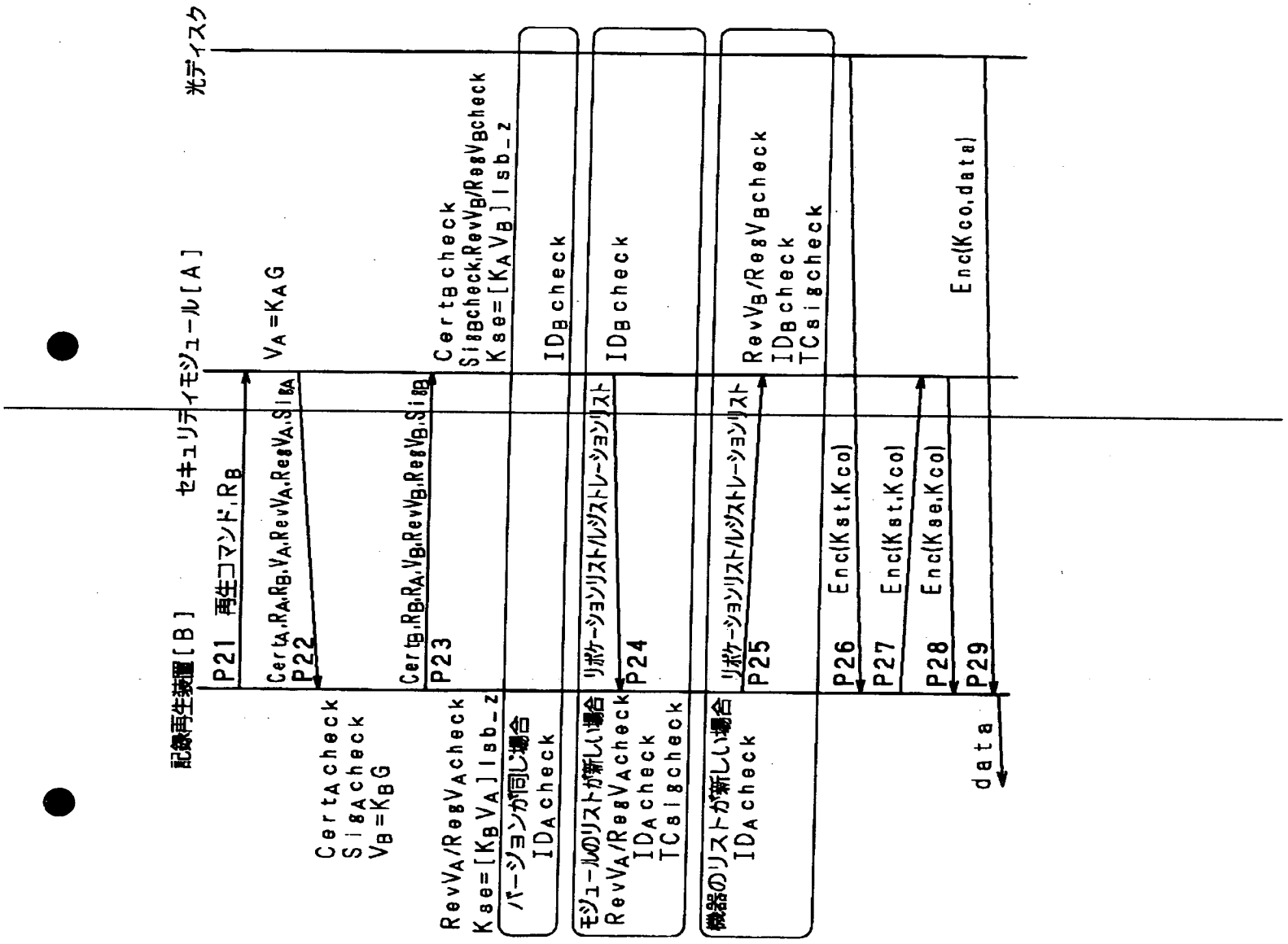
【図４２】


ＩＤ
秘密鍵
公開鍵
公開鍵証明書
リボケーションリスト/レジストレーションリスト
ＩＤ
秘密鍵
公開鍵
公開鍵証明書
リボケーションリスト/レジストレーションリスト
光ディスク
セキュリティモジュール
記録再生装置
再生コマンド
Recording-ID
P1
相互認証
Kse共有
バージョンナンバー
P2
リボケーションリスト/レジストレーションリスト
P3
P4
Enc(Kse,Kco)
P5
Enc(Kco,data)
P6
data

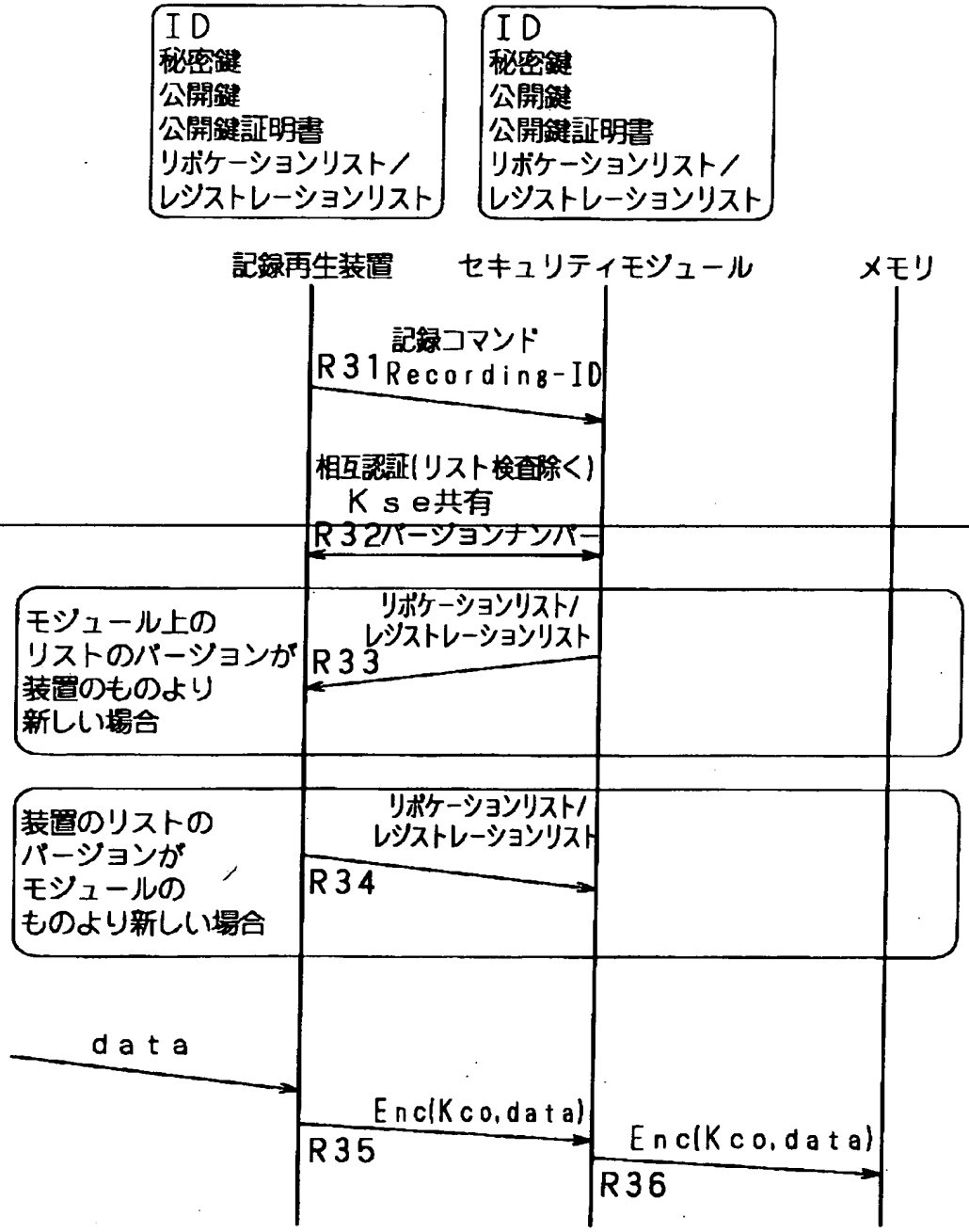
【図４３】


光ディスク
セキュリティモジュール[A]
記録再生装置[B]
P11 再生コマンド,RB
VA=KAG
CertA,RA,RB,VA,RevVA,RegVASigBA
P12
CertA check
SigA check
IDA check
VB=KBG
CertB,RB,RA,VB,RevVB,RegVBSigB
P13
CertB check
SigB check
IDB check
Kse=[KAVB]Isb_z
Kse=[KBVA]Isb_z
リボケーションリストレジストレーションリスト
P14
RevVB/RegVB check
TC sig check
P15
RevVA/RegVA check
TC sig check
P16 Enc(Kst,Kco)
P17 Enc(Kst,Kco)
P18 Enc(Kse,Kco)
P19 Enc(Kco,data)
data

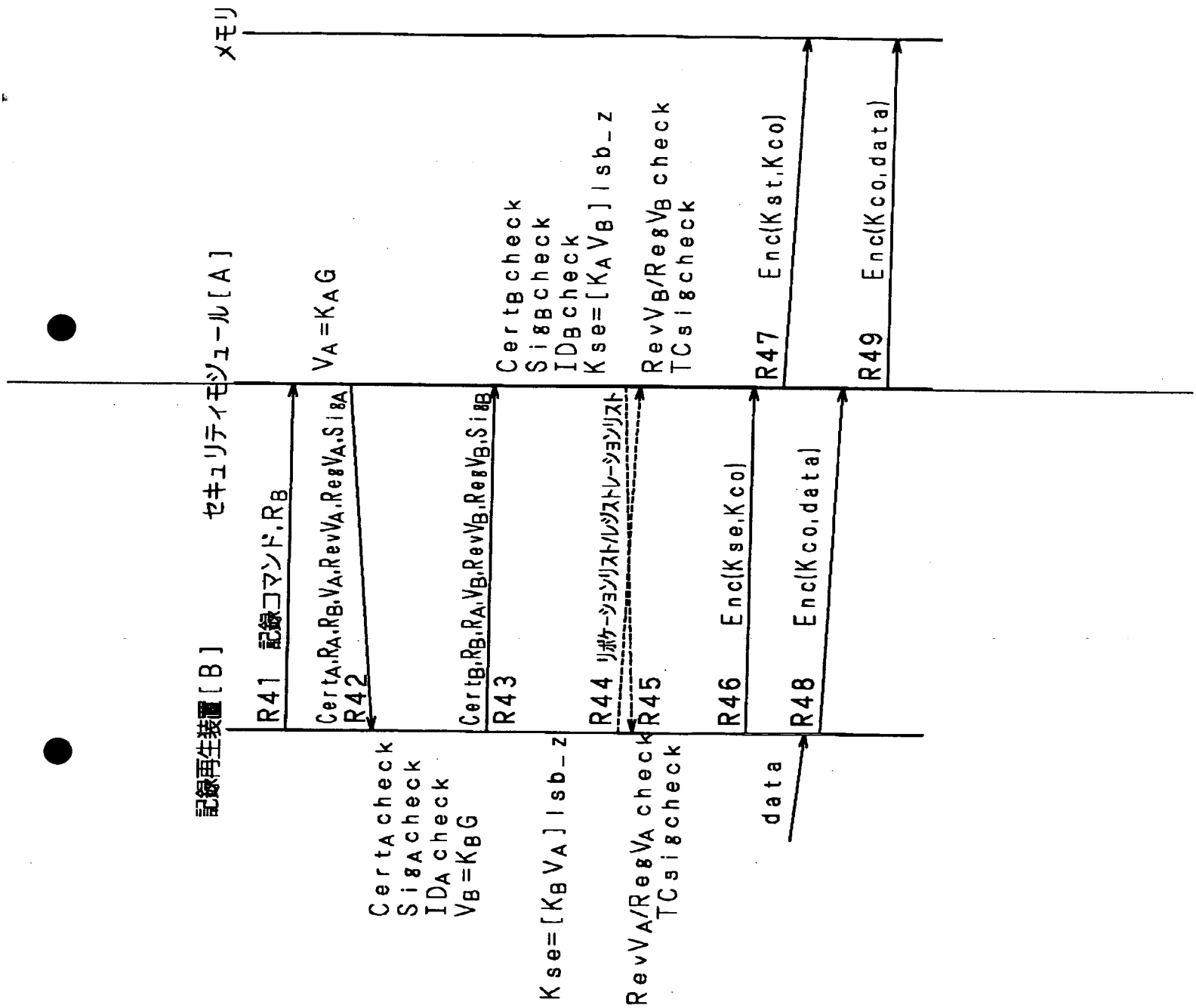
【図４４】


記録再生装置[B]
セキュリティモジュール[A]
光ディスク
P21 再生コマンド:RB
CertA,RA,RB,VA,RevVA,RegVA,SigA
VA=KAG
P22
CertB,RB,RA,VB,RevVB,RegVB,SigB
CertBcheck
SigBcheck,RevVB/RegVBcheck
Kse=[KAVB]lsb_z
IDBcheck
P23
CertAcheck
SigAcheck
VB=KBG
RevVA/RegVAcheck
Kse=[KBVA]lsb_z
バージョンが同じ場合
IDAcheck
モジュールのリストが新しい場合
RevVA/RegVAcheck
IDAcheck
TCsigcheck
リボケーションリストルジストレーションリスト
P24
IDBcheck
機器のリストが新しい場合
IDAcheck
リボケーションリストルジストレーションリスト
P25
RevVB/RegVBcheck
IDBcheck
TCsigcheck
P26 Enc(Kst,Kcol)
P27 Enc(Kst,Kcol)
P28 Enc(Kse,Kcol)
P29
Enc(Kco,data)
data

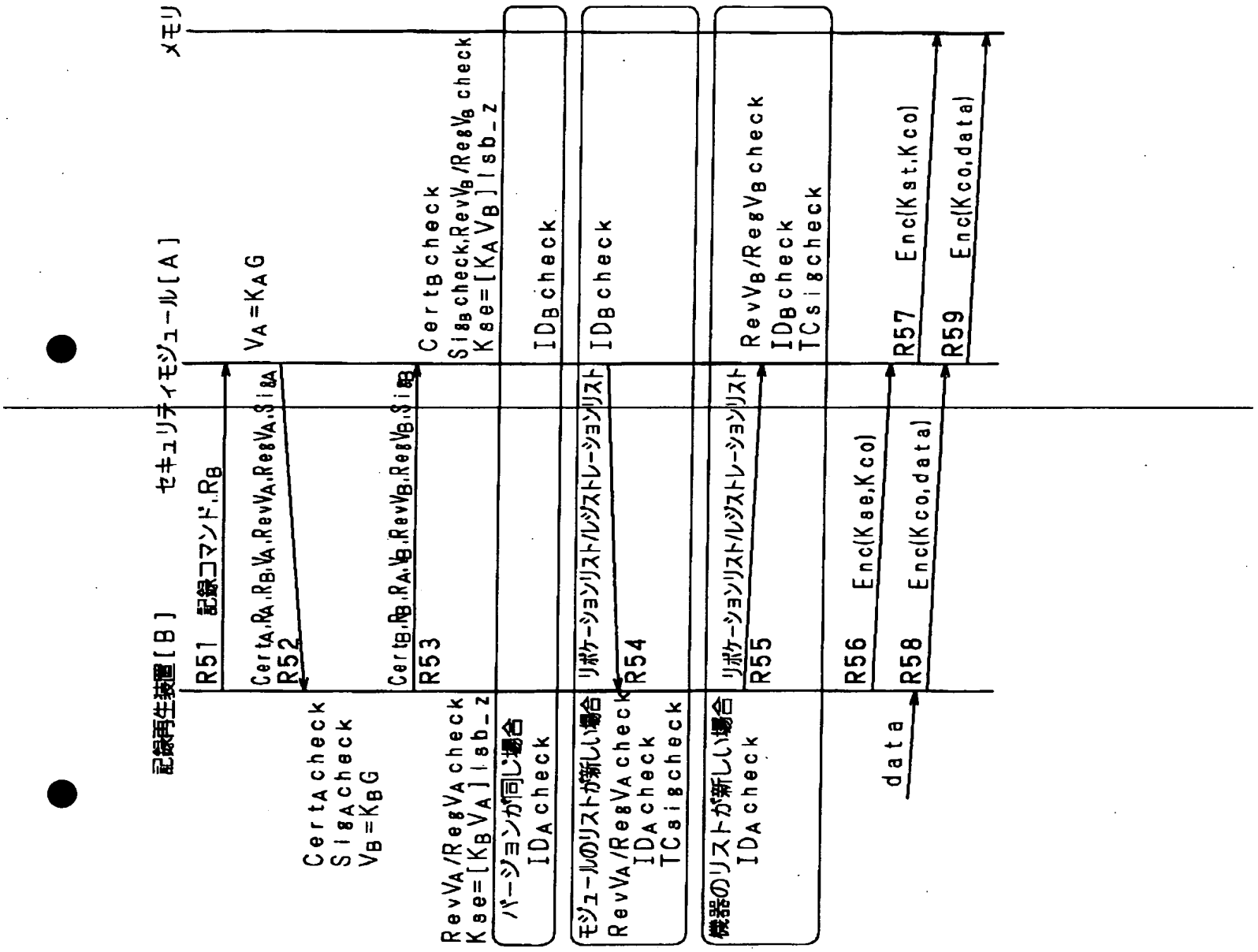
【図４５】


ＩＤ
秘密鍵
公開鍵
公開鍵証明書
リポケーションリスト／
レジストレーションリスト
ＩＤ
秘密鍵
公開鍵
公開鍵証明書
リポケーションリスト／
レジストレーションリスト
記録再生装置
セキュリティモジュール
メモリ
記録コマンド
R31 Recording-ID
相互認証(リスト検査除く)
Ｋｓｅ共有
R32 バージョンナンバー
モジュール上の
リストのバージョンが
装置のものより
新しい場合
リポケーションリスト/
レジストレーションリスト
R33
装置のリストの
バージョンが
モジュールの
ものより新しい場合
リポケーションリスト/
レジストレーションリスト
R34
ｄａｔａ
Enc(Kco,data)
R35
Enc(Kco,data)
R36

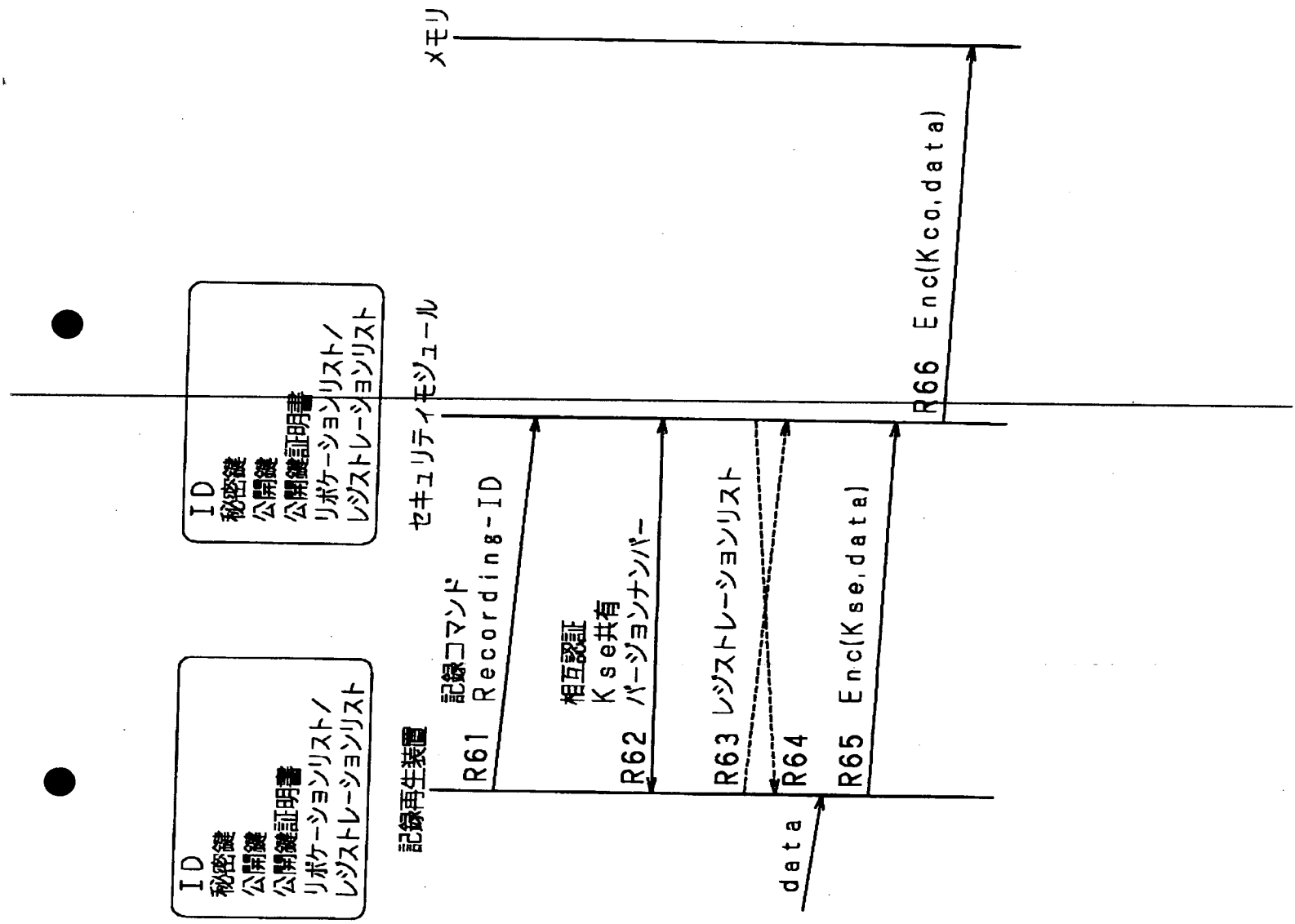
【図４６】


メモリ
セキュリティモジュール[A]
記録再生装置[B]
R41 記録コマンド,RB
R42
CertA,RA,RB,VA,RevVA,RegVA,SigA
CertA check
SigA check
IDA check
VB=KBG
R43
CertB,RB,RA,VB,RevVB,RegVB,SigB
Kse=[KBVA]lsb_z
R44 リボケーションリスト/リボケーションリスト
R45
RevVA/RegVA check
TCsigcheck
R46 Enc(Kse,Kcol)
R48 Enc(Kco,data)
data
VA=KAG
CertB check
SigB check
IDB check
Kse=[KAVB]lsb_z
RevVB/RegVB check
TCsigcheck
R47 Enc(Kst,Kcol)
R49 Enc(Kco,data)

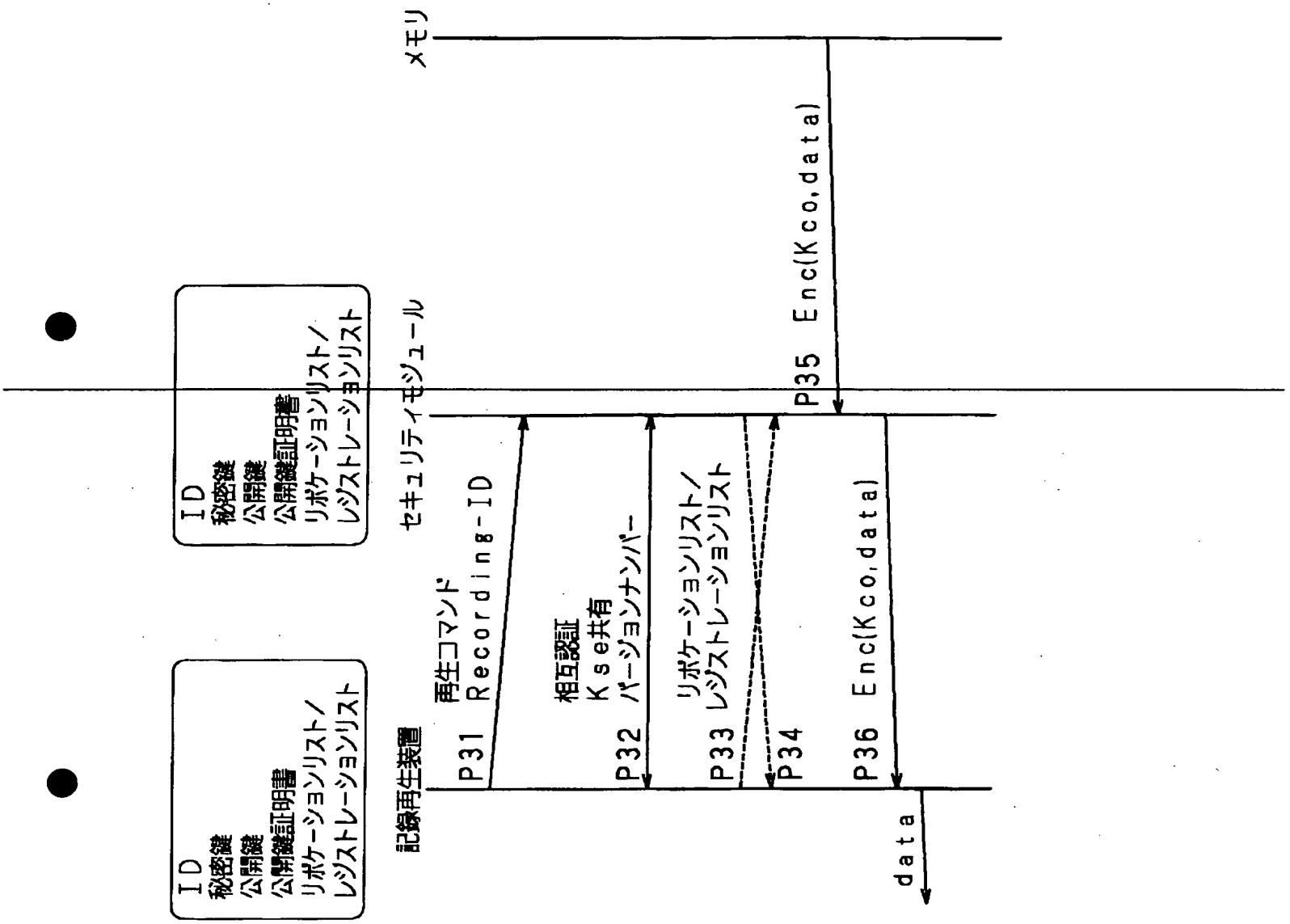
【図４７】


記録再生装置[B]
セキュリティモジュール[A]
メモリ
R51 記録コマンド,RB
VA=KAG
R52
CertA,RA,RB,VA,RevVA,RegVA,SigA
CertA check
SigA check
VB=KBG
R53
CertB,RB,RA,VB,RevVB,RegVB,SigB
RevVA/RegVA check
Kse=[KBVA]Isb_z
CertB check
SigB check,RevVB/RegVB check
Kse=[KAVB]Isb_z
バージョンが同じ場合
IDA check
IDB check
リボケーションリスト/リジストレーションリスト
R54
モジュールのリストが新しい場合
RevVA/RegVA check
IDA check
TCsig check
IDB check
リボケーションリスト/リジストレーションリスト
R55
機器のリストが新しい場合
IDA check
RevVB/RegVB check
IDB check
TCsig check
R56 Enc(Kse,Kco)
R57 Enc(Kst,Kco)
R58 Enc(Kco,data)
R59 Enc(Kco,data)
data

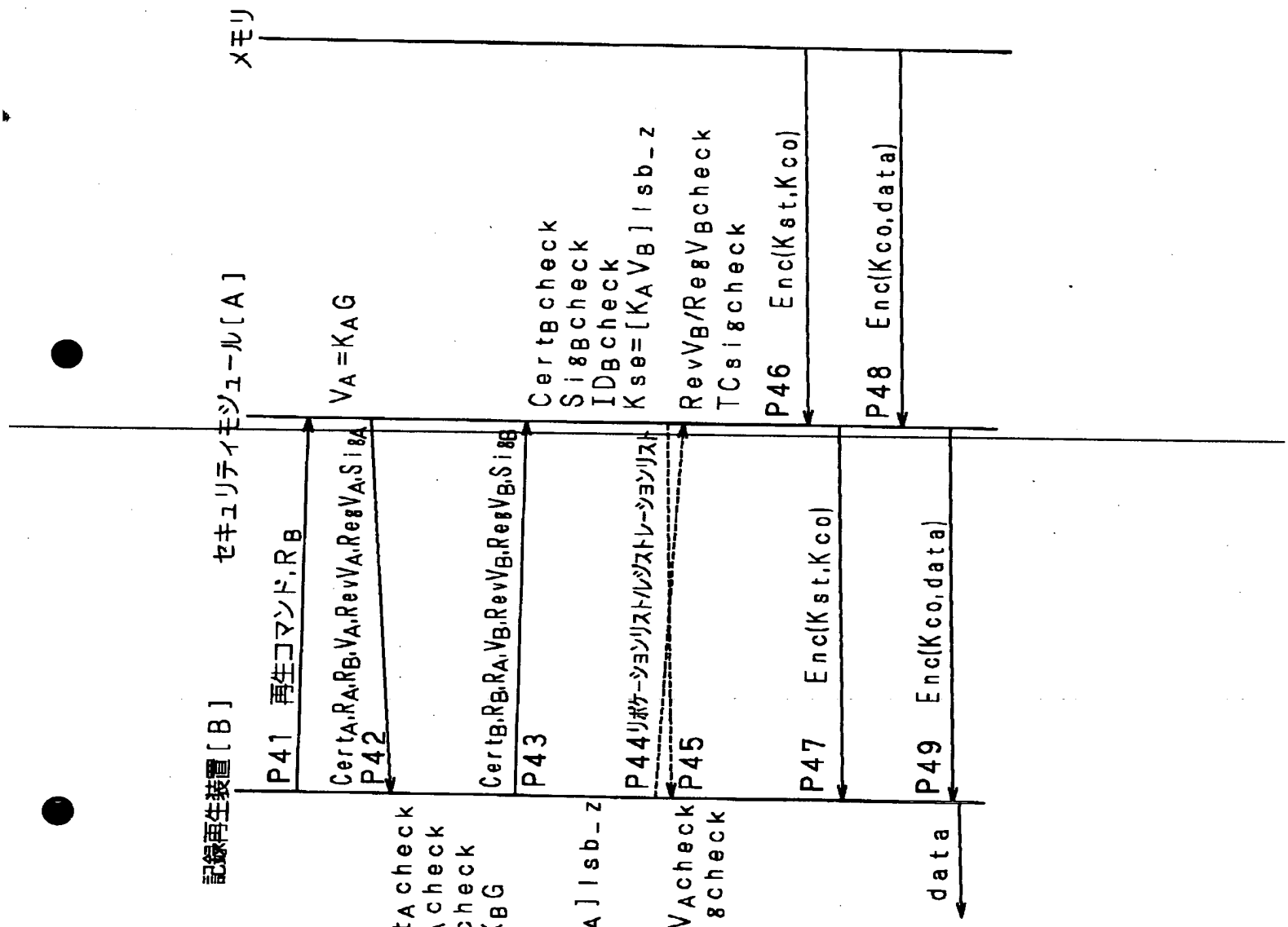
【図４８】


メモリ
セキュリティモジュール
ID
秘密鍵
公開鍵
公開鍵証明書
リボケーションリスト／
レジストレーションリスト
ID
秘密鍵
公開鍵
公開鍵証明書
リボケーションリスト／
レジストレーションリスト
記録再生装置
記録コマンド
R61 Recording-ID
相互認証
Kse共有
R62 バージョンナンバー
R63 レジストレーションリスト
R64
R65 Enc(Kse,data)
R66 Enc(Kco,data)
data

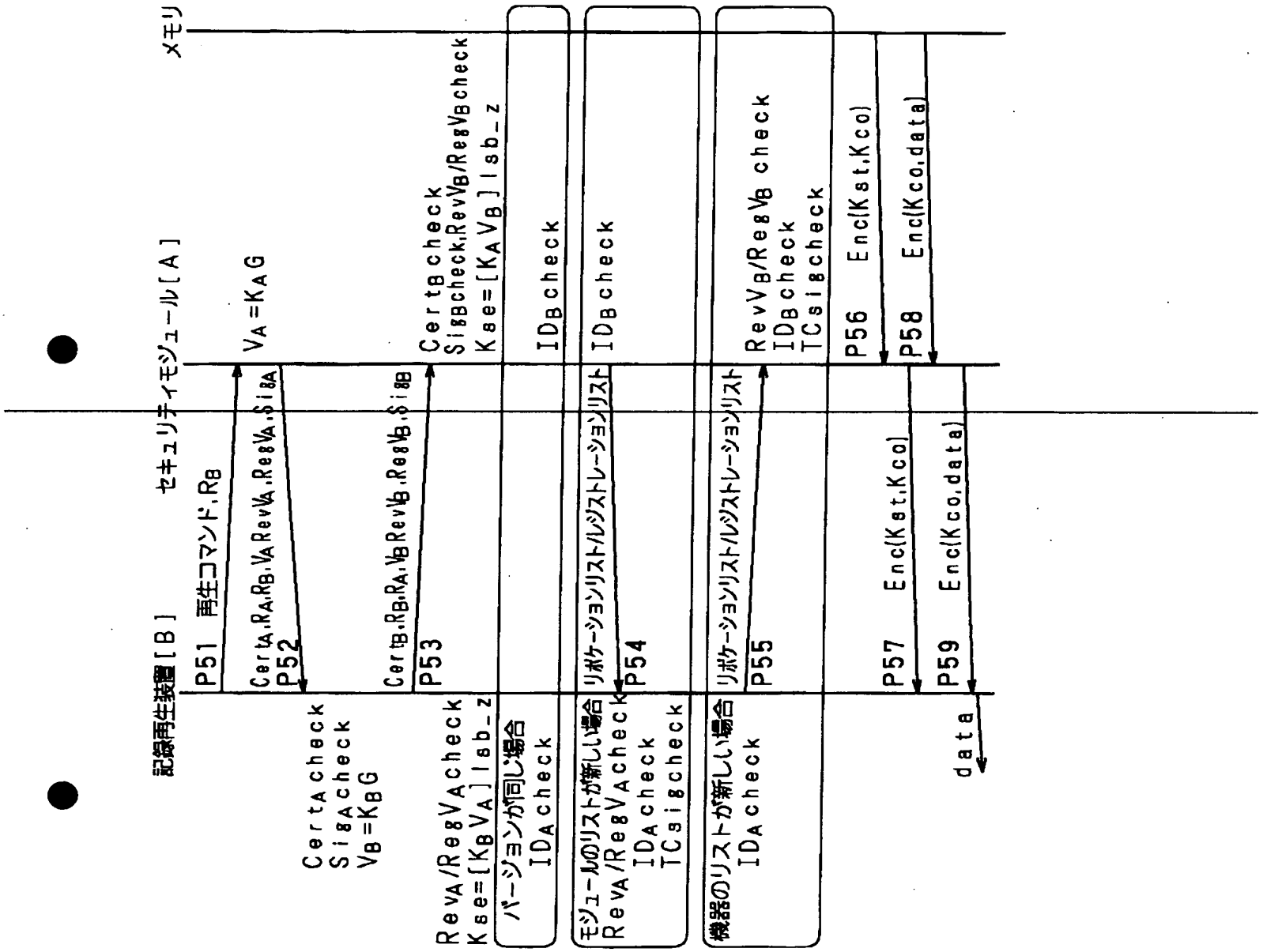
【図４９】


メモリ
セキュリティモジュール
記録再生装置
ID
秘密鍵
公開鍵
公開鍵証明書
リボケーションリスト／
レジストレーションリスト
ID
秘密鍵
公開鍵
公開鍵証明書
リボケーションリスト／
レジストレーションリスト
再生コマンド
P31 Recording-ID
相互認証
Kse共有
P32 バージョンナンバー
リボケーションリスト／
P33 レジストレーションリスト
P34
P35 Enc(Kco,data)
P36 Enc(Kco,data)
data

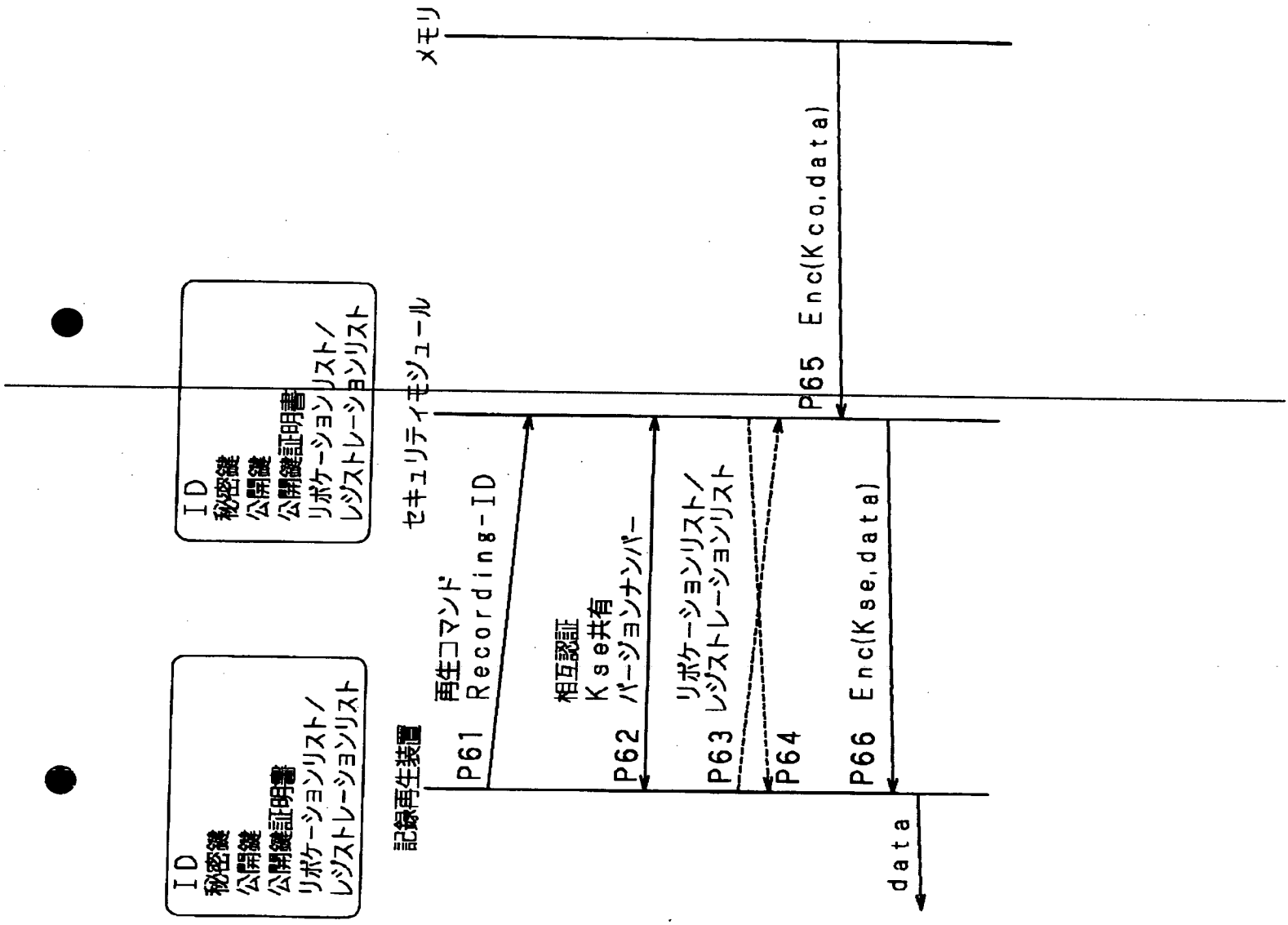
【図５０】


メモリ
セキュリティモジュール［A］
記録再生装置［B］
P41 再生コマンド,RB
CertA,RA,RB,VA,RevVA,RegVA,SigA
P42
CertB,RB,RA,VB,RevVB,RegVB,SigB
P43
P44 リボケーションリストレジストレーションリスト
P45
P46 Enc(Kst,Kco)
P47 Enc(Kst,Kco)
P48 Enc(Kco,data)
P49 Enc(Kco,data)
VA=KAG
CertB check
SigB check
IDB check
Kse=[KAVB]Isb_z
RevVB/RegVB check
TCsig check
CertA check
SigA check
IDA check
VB=KBG
Kse=[KBVA]Isb_z
RevVA/RegVA check
TCsig check
data

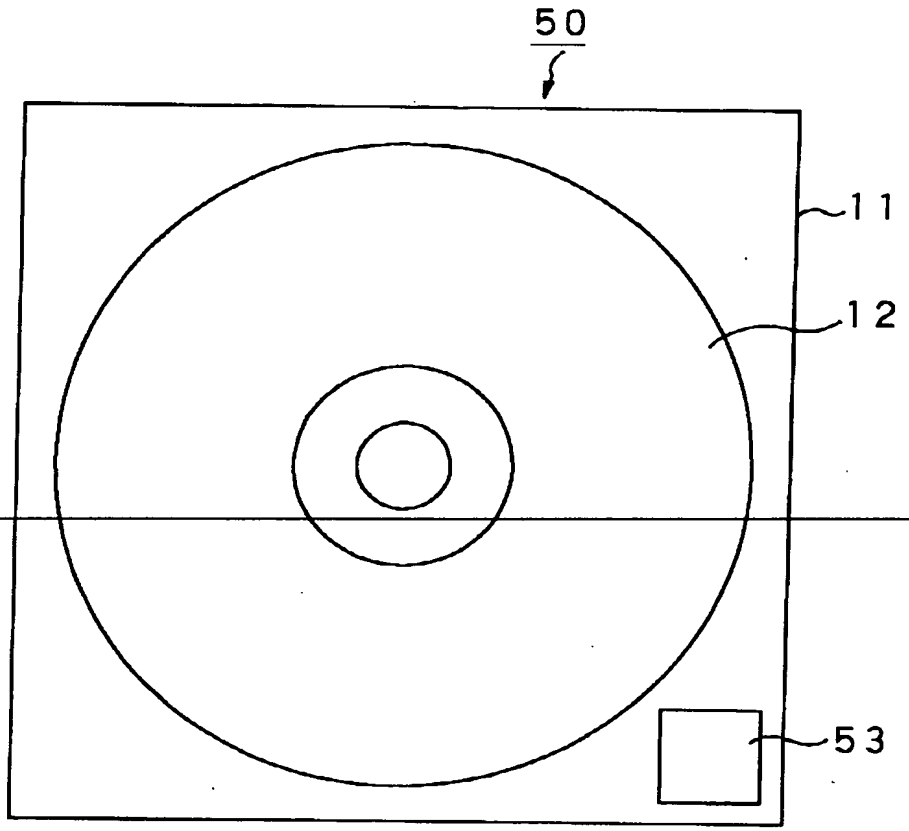
【図５１】


記録再生装置[B]
セキュリティモジュール[A]
メモリ
P51 再生コマンド,RB
CertA,RA,RB,VA RevVA,RegVA,$iBA
P52
CertB,RB,RA,VB RevVB,RegVB,$iBB
P53
P54
P55
P56 Enc(Kst,Kco)
P57 Enc(Kst,Kco)
P58 Enc(Kco,data)
P59 Enc(Kco,data)
VA=KAG
CertA check
SigA check
VB=KBG
RevA/RegVA check
Kse=[KBVA]Isb_z
CertB check
SigBcheck,RevVB/RegVB check
Kse=[KAVB]Isb_z
IDB check
バージョンが同じ場合
IDA check
IDB check
モジュールのリストが新しい場合
RevA/RegVA check
IDA check
TCsigcheck
RevVB/RegVB check
IDB check
TCsigcheck
機器のリストが新しい場合
IDA check
data

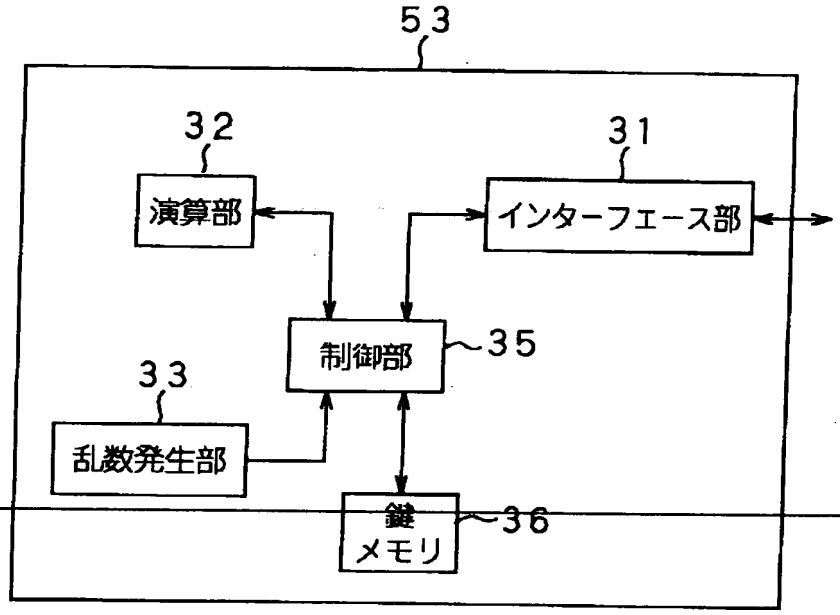
【図５２】


メモリ
ID
秘密鍵
公開鍵
公開鍵証明書
リボケーションリスト／
レジストレーションリスト
セキュリティモジュール
ID
秘密鍵
公開鍵
公開鍵証明書
リボケーションリスト／
レジストレーションリスト
記録再生装置
P61 再生コマンド Recording-ID
相互認証
Kse共有
P62 バージョンナンバー
リボケーションリスト／
P63 レジストレーションリスト
P64
P65 Enc(Kco,data)
P66 Enc(Kse,data)
data

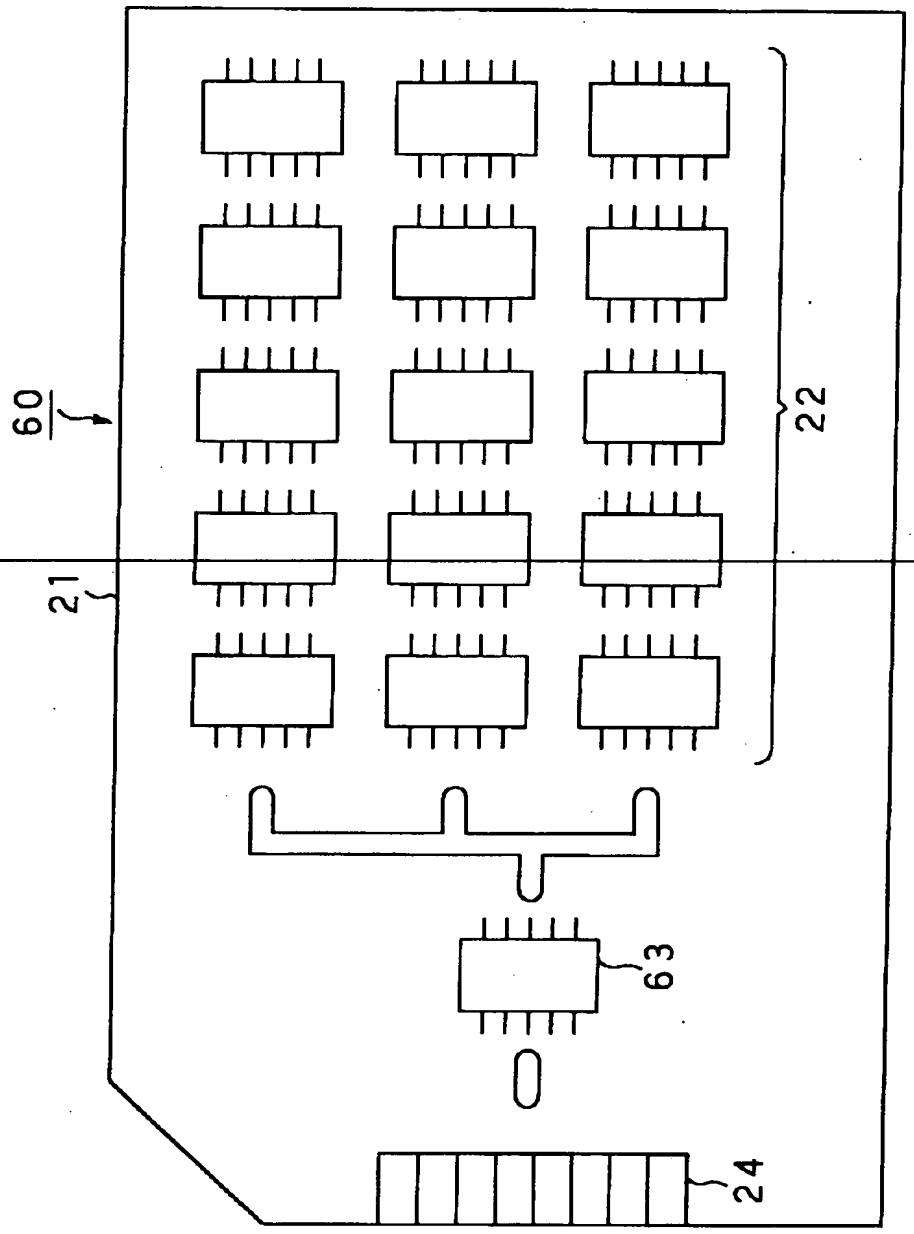
【図５３】



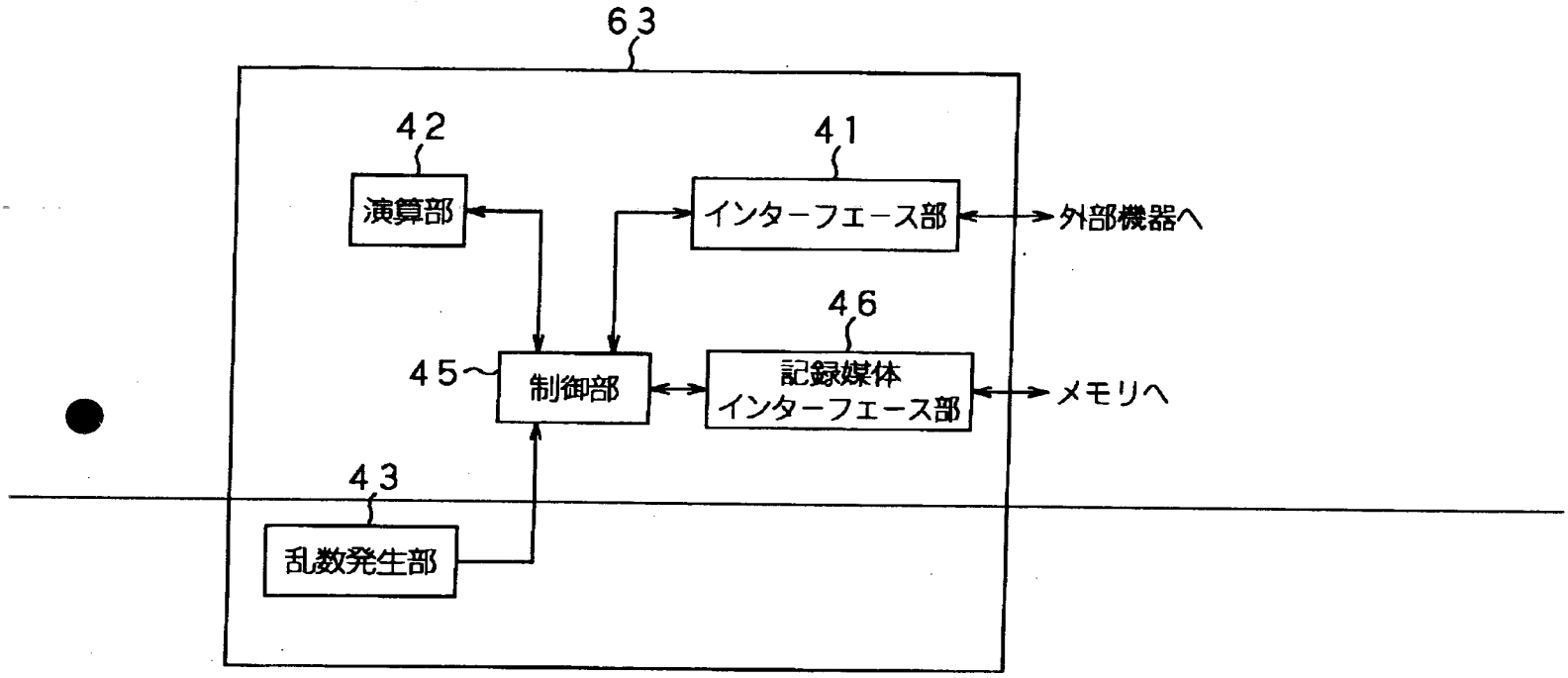
【図５４】



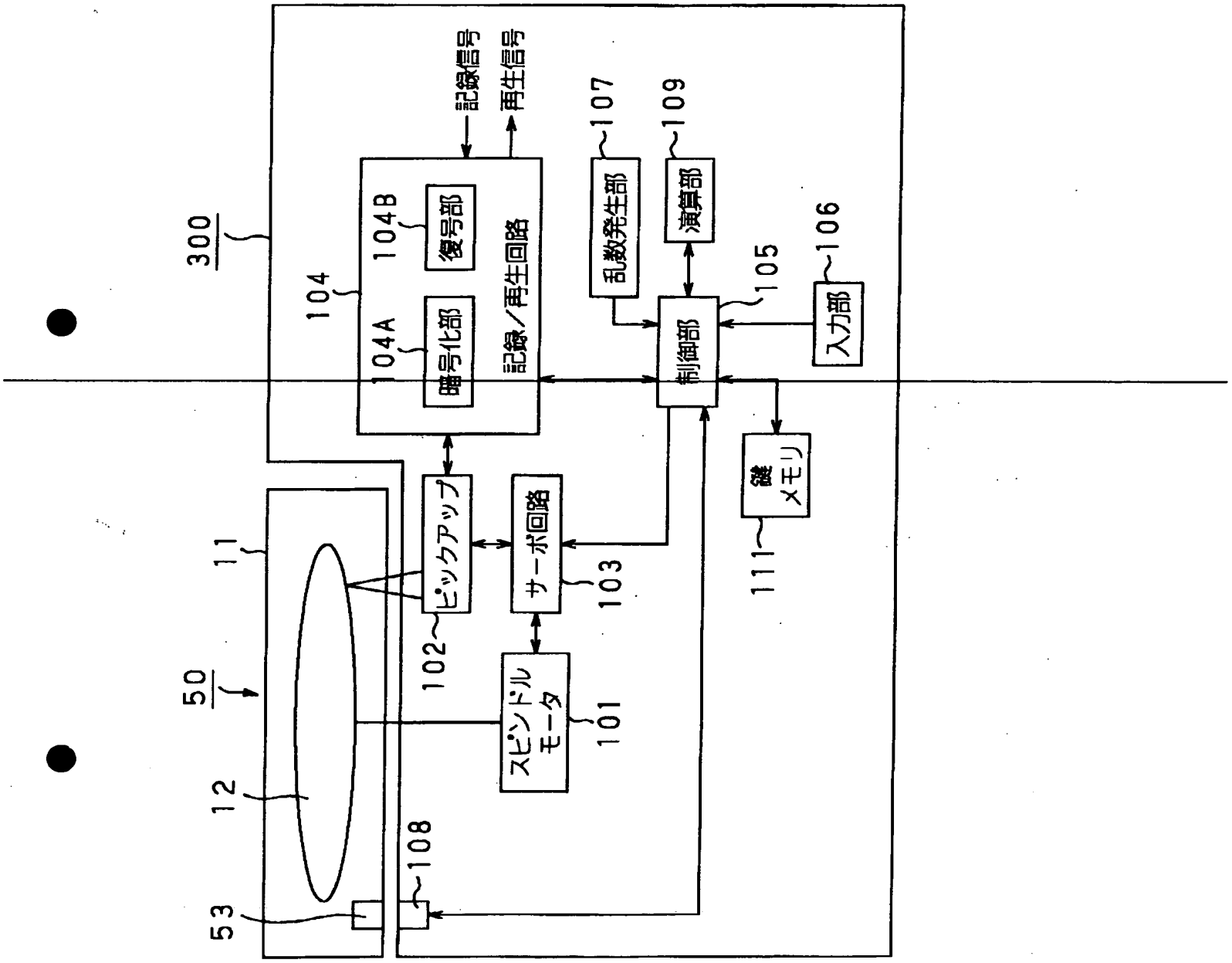
【図５５】



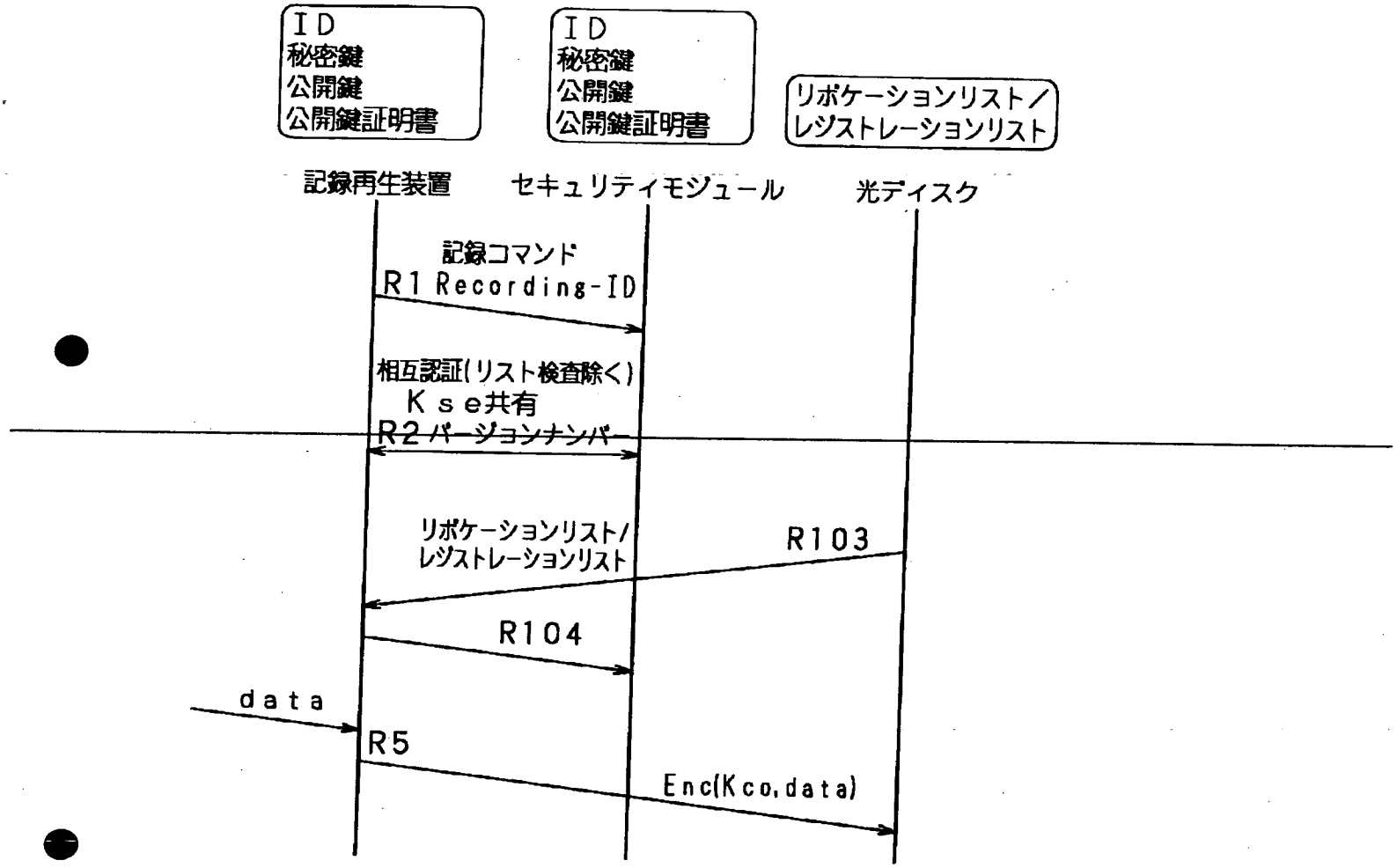
【図５６】


63
42
41
演算部
インターフェース部
外部機器へ
46
45
制御部
記録媒体
インターフェース部
メモリへ
43
乱数発生部

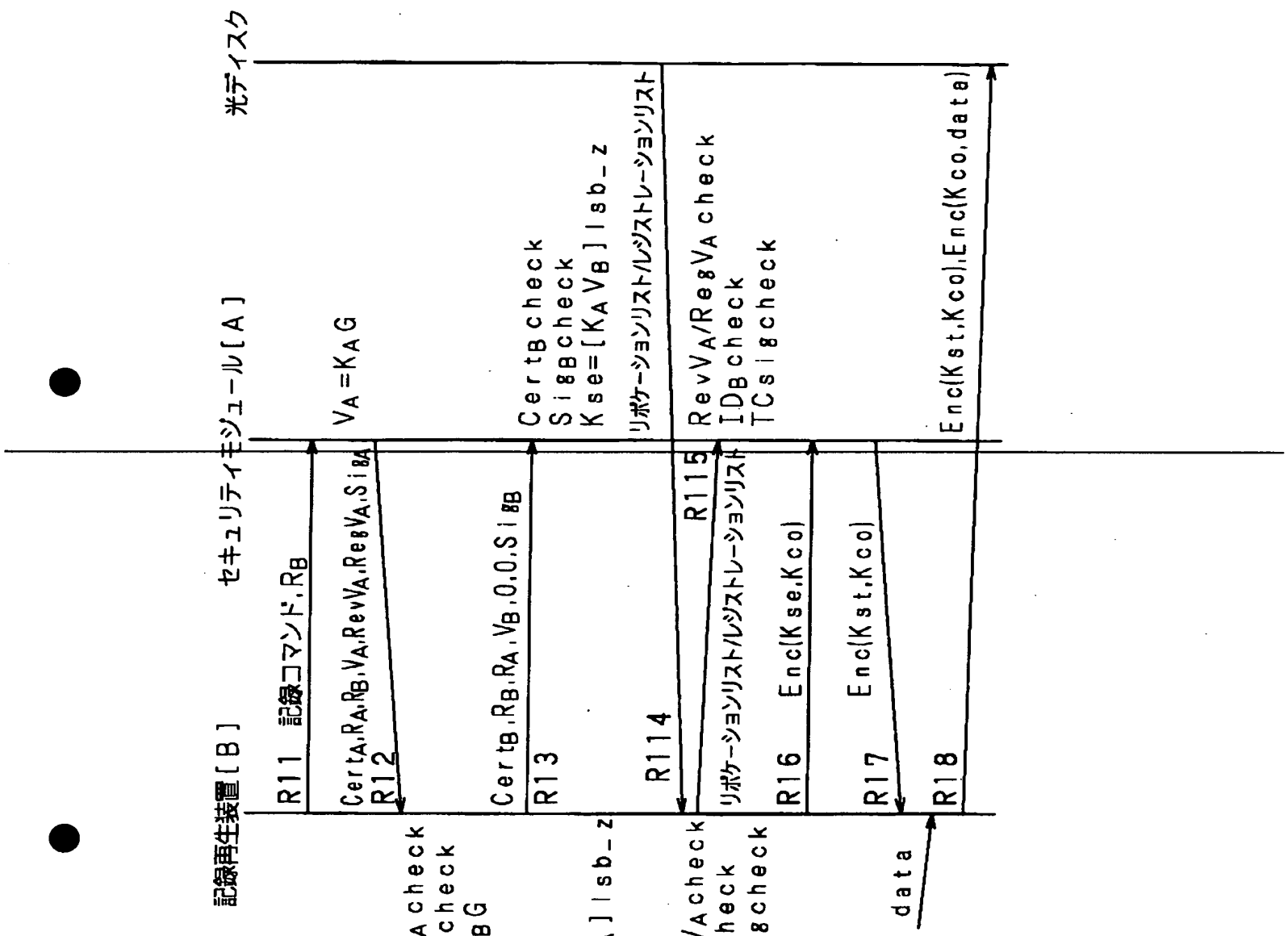
【図５７】


300
104
104A
暗号化部
104B
復号部
記録／再生回路
記録信号
再生信号
107
乱数発生部
109
演算部
105
制御部
106
入力部
111
鍵メモリ
11
ピックアップ
102
サーボ回路
103
スピンドルモータ
101
50
12
53
108

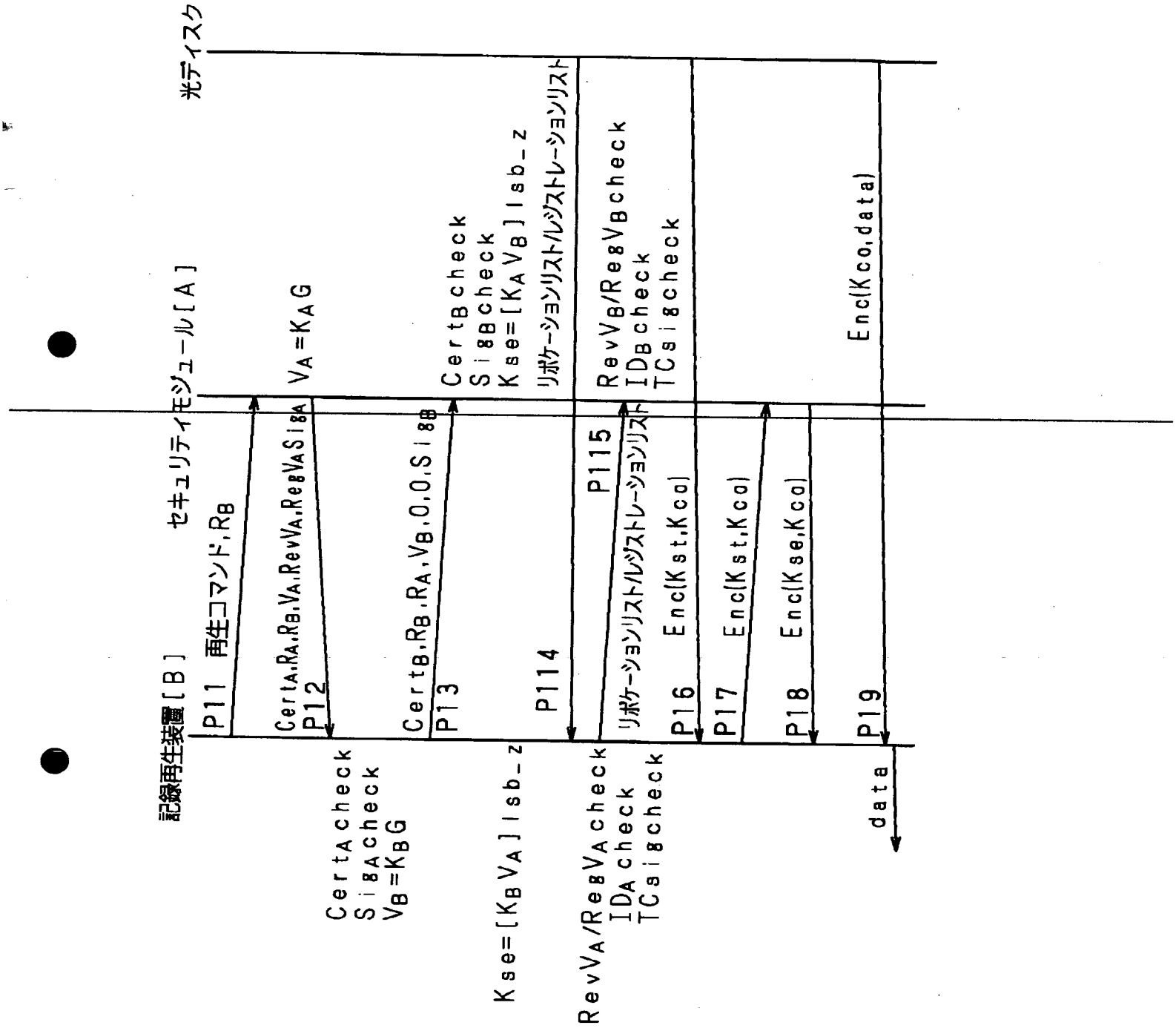
【図５８】


ＩＤ
秘密鍵
公開鍵
公開鍵証明書
ＩＤ
秘密鍵
公開鍵
公開鍵証明書
リボケーションリスト／
レジストレーションリスト
記録再生装置
セキュリティモジュール
光ディスク
記録コマンド
R1 Recording-ID
相互認証(リスト検査除く)
Ｋｓｅ共有
R2 バージョンナンバー
リボケーションリスト/
レジストレーションリスト
R103
R104
data
R5
Enc(Kco,data)

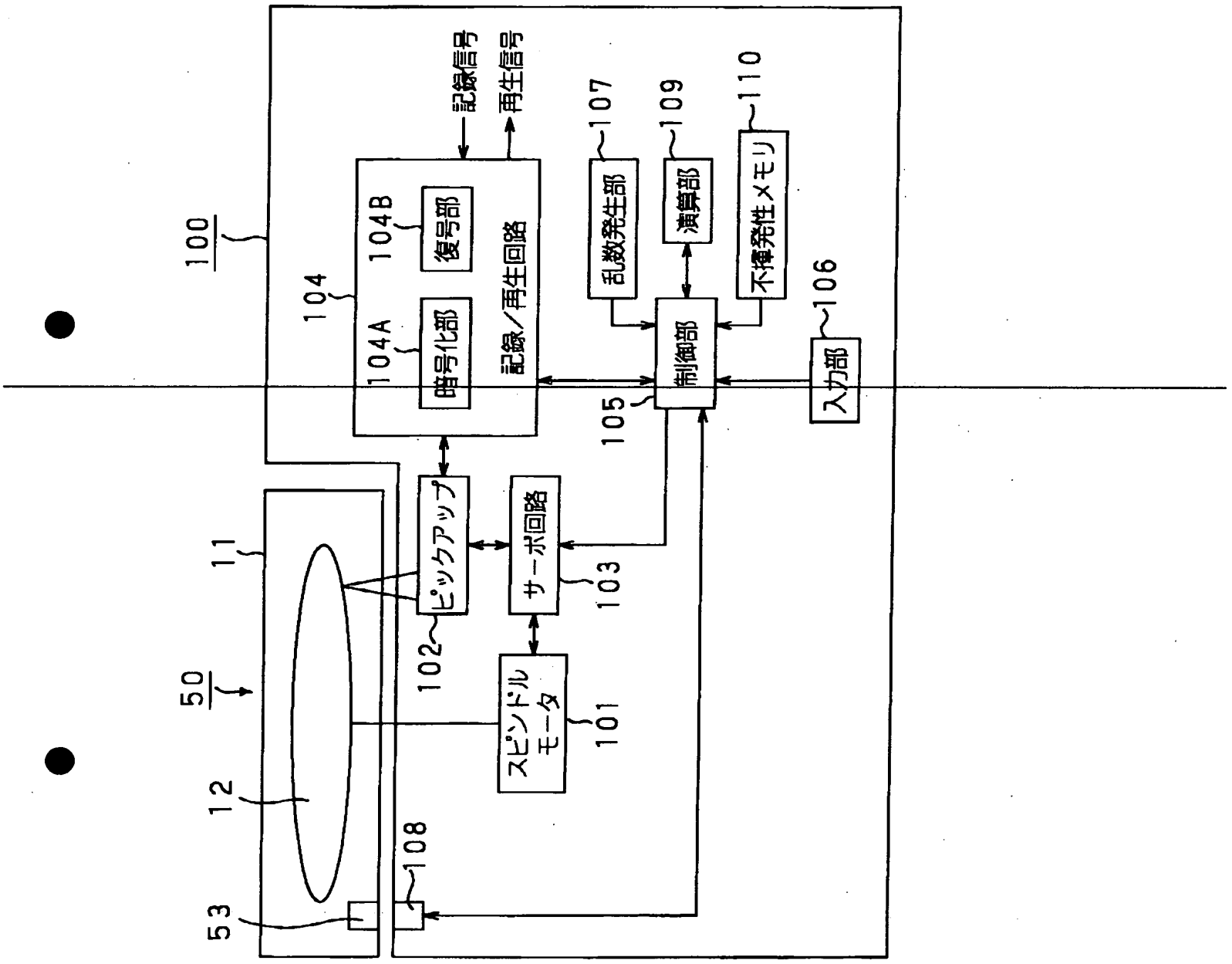
【図５９】


光ディスク
セキュリティモジュール[A]
記録再生装置[B]
R11 記録コマンド,RB
VA=KAG
CertA,RA,RB,VA,RevVA,RegVA,SigA
R12
CertA check
SigA check
VB=KBG
CertB,RB,RA,VB,0,0,SigB
R13
CertB check
SigB check
Kse=[KAVB]lsb_z
R114
リボケーションリストレジストレーションリスト
R115
RevVA/RegVA check
IDB check
TCsigcheck
Kse=[KBVA]lsb_z
RevVA/RegVA check
IDA check
TCsigcheck
R16 Enc(Kse,Kco)
R17 Enc(Kst,Kco)
R18 Enc(Kst,Kco),Enc(Kco,data)
data

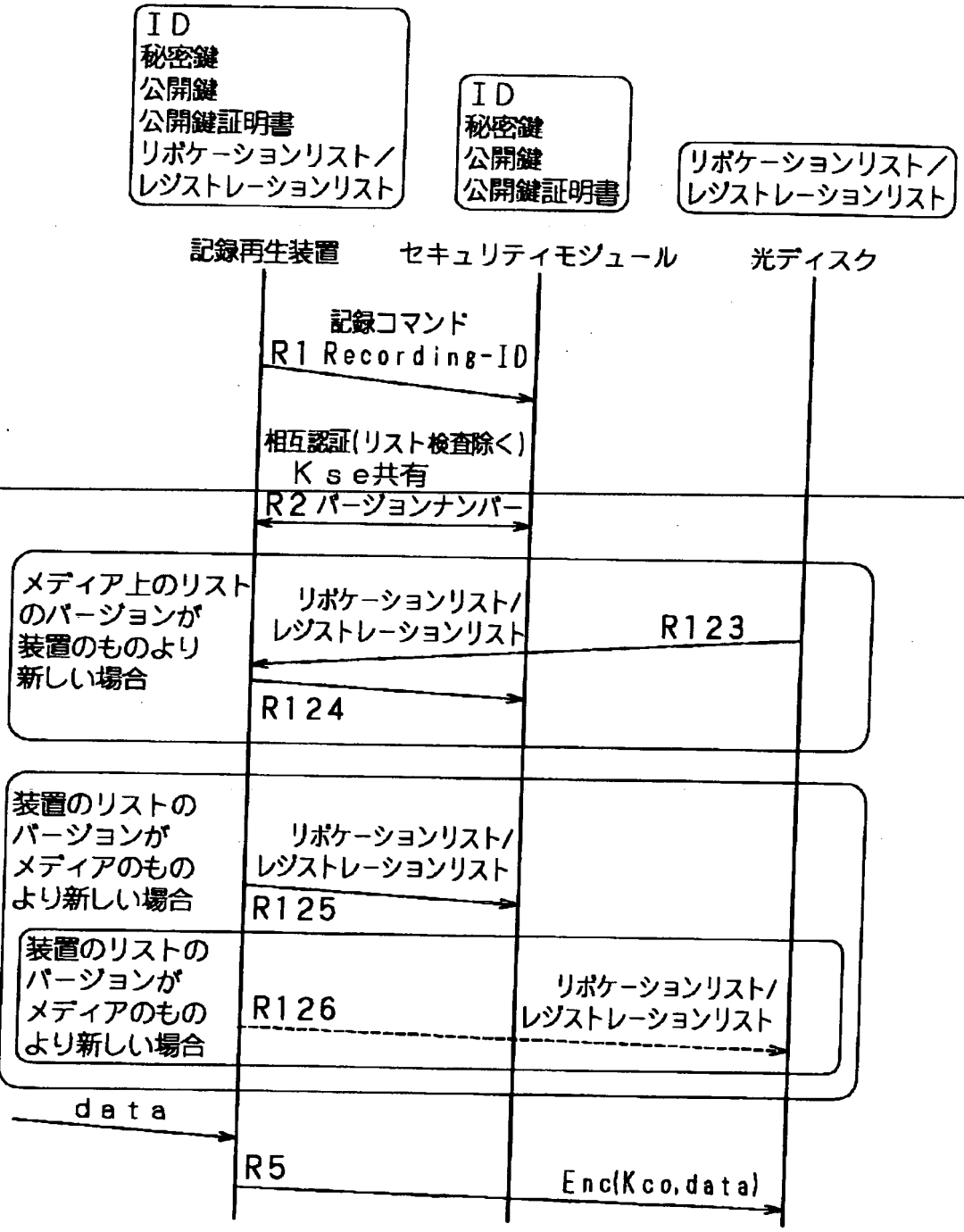
【図６０】


光ディスク
セキュリティモジュール[A]
記録再生装置[B]
P11 再生コマンド,RB
CertA,RA,RB,VA,RevVA,RegVA,SigA
P12
CertA check
SigA check
VB=KBG
CertB,RB,RA,VB,0,0,SigB
P13
CertB check
SigB check
Kse=[KAVB]Isb_z
リボケーションリスト/リジストレーションリスト
P114
Kse=[KBVA]Isb_z
P115
RevVB/RegVB check
IDB check
TCsig check
リボケーションリスト/リジストレーションリスト
RevVA/RegVA check
IDA check
TCsig check
P16 Enc(Kst,Kco)
P17 Enc(Kst,Kco)
P18 Enc(Kse,Kco)
P19 Enc(Kco,data)
data

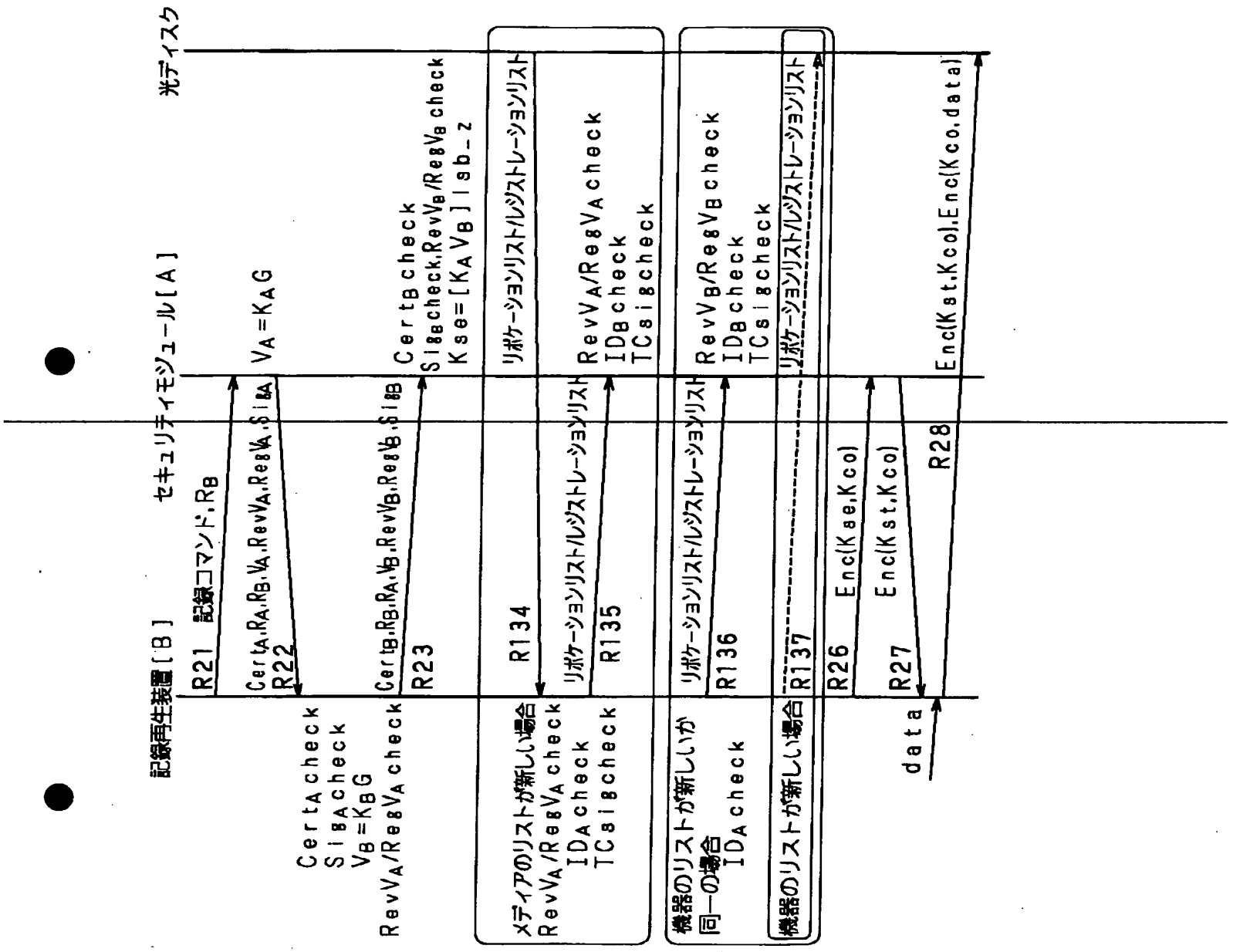
【図６１】


100
104
104A
暗号化部
104B
復号部
記録／再生回路
記録信号
再生信号
107
乱数発生部
109
演算部
110
不揮発性メモリ
106
入力部
制御部
105
ピックアップ
102
サーボ回路
103
スピンドルモータ
101
11
50
12
53
108

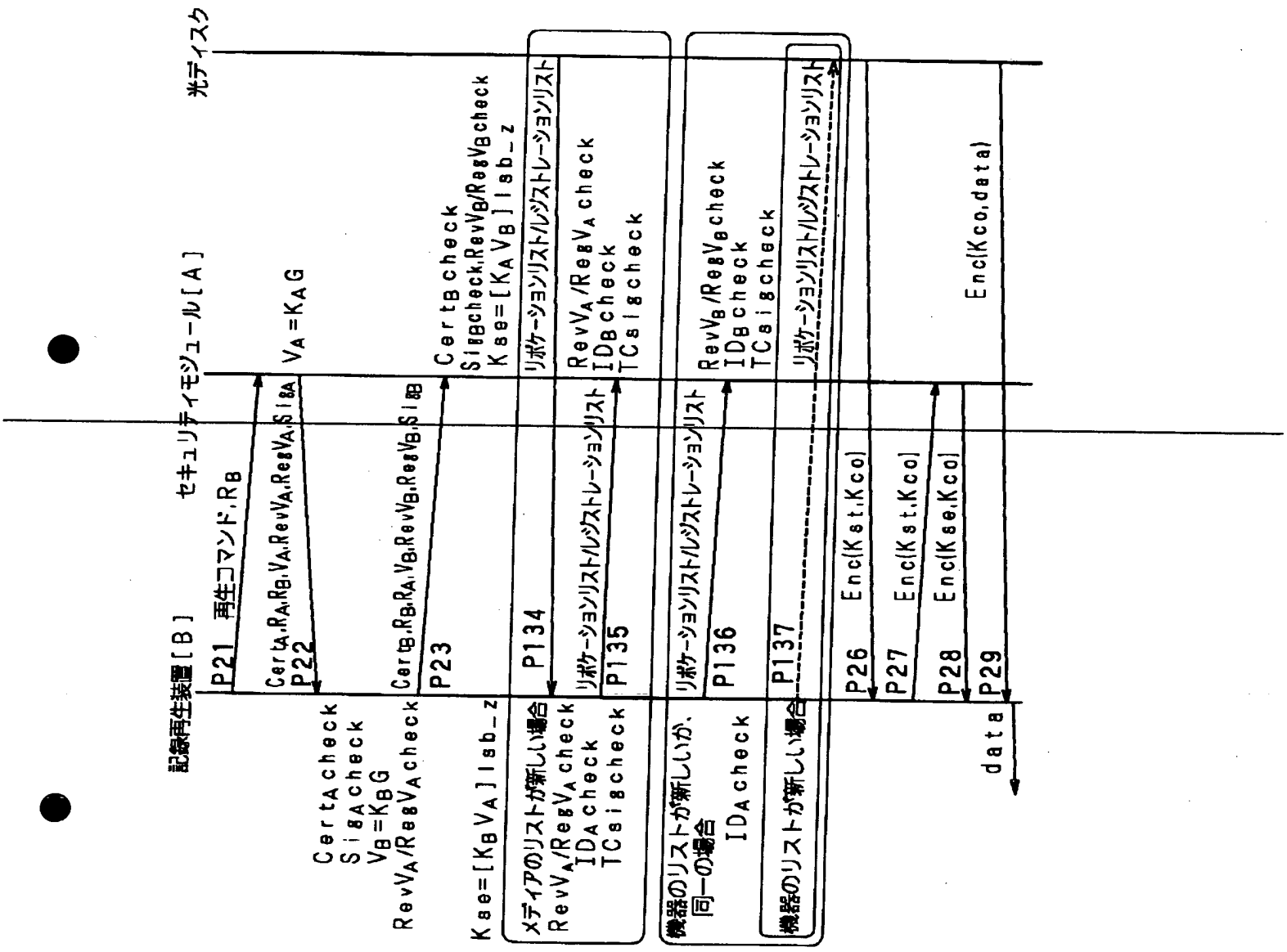
【図６２】


ＩＤ
秘密鍵
公開鍵
公開鍵証明書
リボケーションリスト／
レジストレーションリスト
ＩＤ
秘密鍵
公開鍵
公開鍵証明書
リボケーションリスト／
レジストレーションリスト
記録再生装置
セキュリティモジュール
光ディスク
記録コマンド
R1 Recording-ID
相互認証(リスト検査除く)
Ｋｓｅ共有
R2 バージョンナンバー
メディア上のリスト
のバージョンが
装置のものより
新しい場合
リボケーションリスト／
レジストレーションリスト
R123
R124
装置のリストの
バージョンが
メディアのもの
より新しい場合
リボケーションリスト／
レジストレーションリスト
R125
装置のリストの
バージョンが
メディアのもの
より新しい場合
R126
リボケーションリスト／
レジストレーションリスト
ｄａｔａ
R5
Enc(Kco,data)

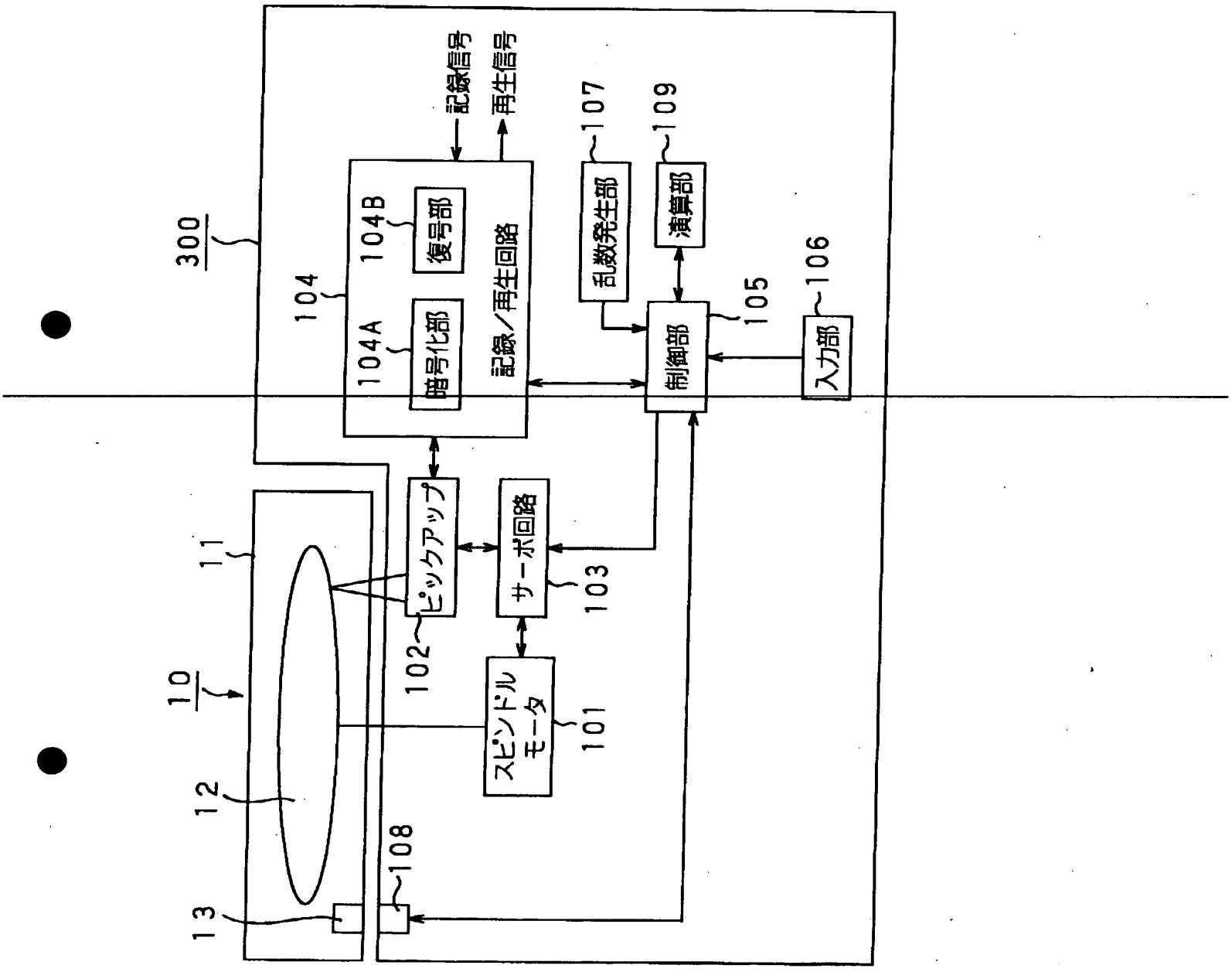
【図６３】


光ディスク
セキュリティモジュール[A]
記録再生装置[B]
R21 記録コマンド,RB
CertA,RA,RB,VA,RevVA,RegVA,SigA
R22
VA=KAG
CertB,RB,RA,VB,RevVB,RegVB,SigB
R23
CertB check
SigB check,RevVB/RegVB check
Kse=[KA VB] lsb_z
R134
リボケーションリスト/レジストレーションリスト
R135
RevVA/RegVA check
IDB check
TCsig check
メディアのリストが新しい場合
RevVA/RegVA check
IDA check
TCsig check
R136
RevVB/RegVB check
IDB check
TCsig check
機器のリストが新しいか同一の場合
IDA check
R137
R26 Enc(Kse,Kcol)
R27 Enc(Kst,Kcol)
R28 Enc(Kst,Kcol),Enc(Kco,data)
CertA check
SigA check
VB=KBG
RevVA/RegVA check
data

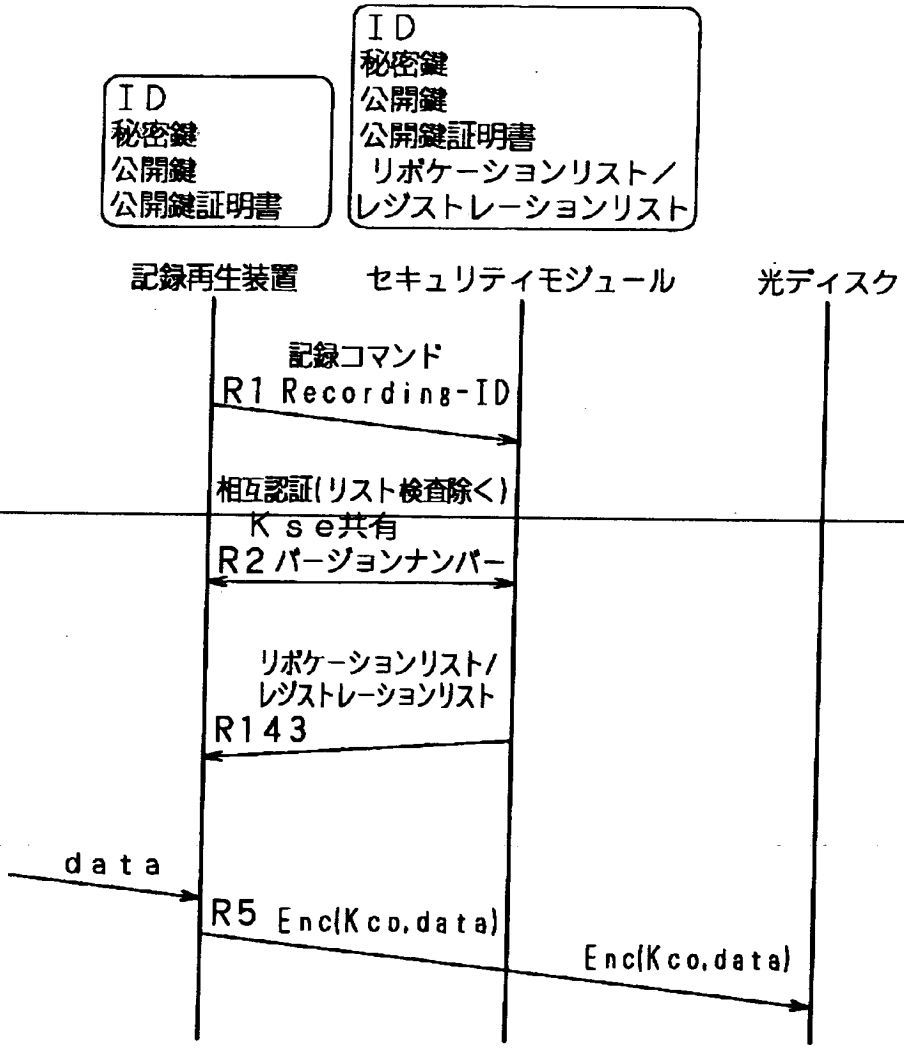
【図６４】


記録再生装置[B]
セキュリティモジュール[A]
光ディスク
P21 再生コマンド,RB
CertA,RA,RB,VA,RevVA,RegVA,SigA
P22
VA=KAG
CertB,RB,RA,VB,RevVB,RegVB,SigB
P23
CertB check
SigBcheck,RevVB/RegVBcheck
Kse=[KA VB]lsb_z
CertA check
SigAcheck
VB=KBG
RevVA/RegVAcheck
Kse=[KB VA]lsb_z
メディアのリストが新しい場合
RevVA/RegVA check
IDA check
TCsigcheck
P134
リボケーションリスト/レジストレーションリスト
リボケーションリスト/レジストレーションリスト
RevVA/RegVA check
IDB check
TCsigcheck
P135
機器のリストが新しいか、同一の場合
IDA check
リボケーションリスト/レジストレーションリスト
RevVB/RegVB check
IDB check
TCsigcheck
P136
機器のリストが新しい場合
リボケーションリスト/レジストレーションリスト
P137
P26 Enc(Kst,Kco)
P27 Enc(Kst,Kco)
P28 Enc(Kse,Kco)
P29 Enc(Kco,data)
data

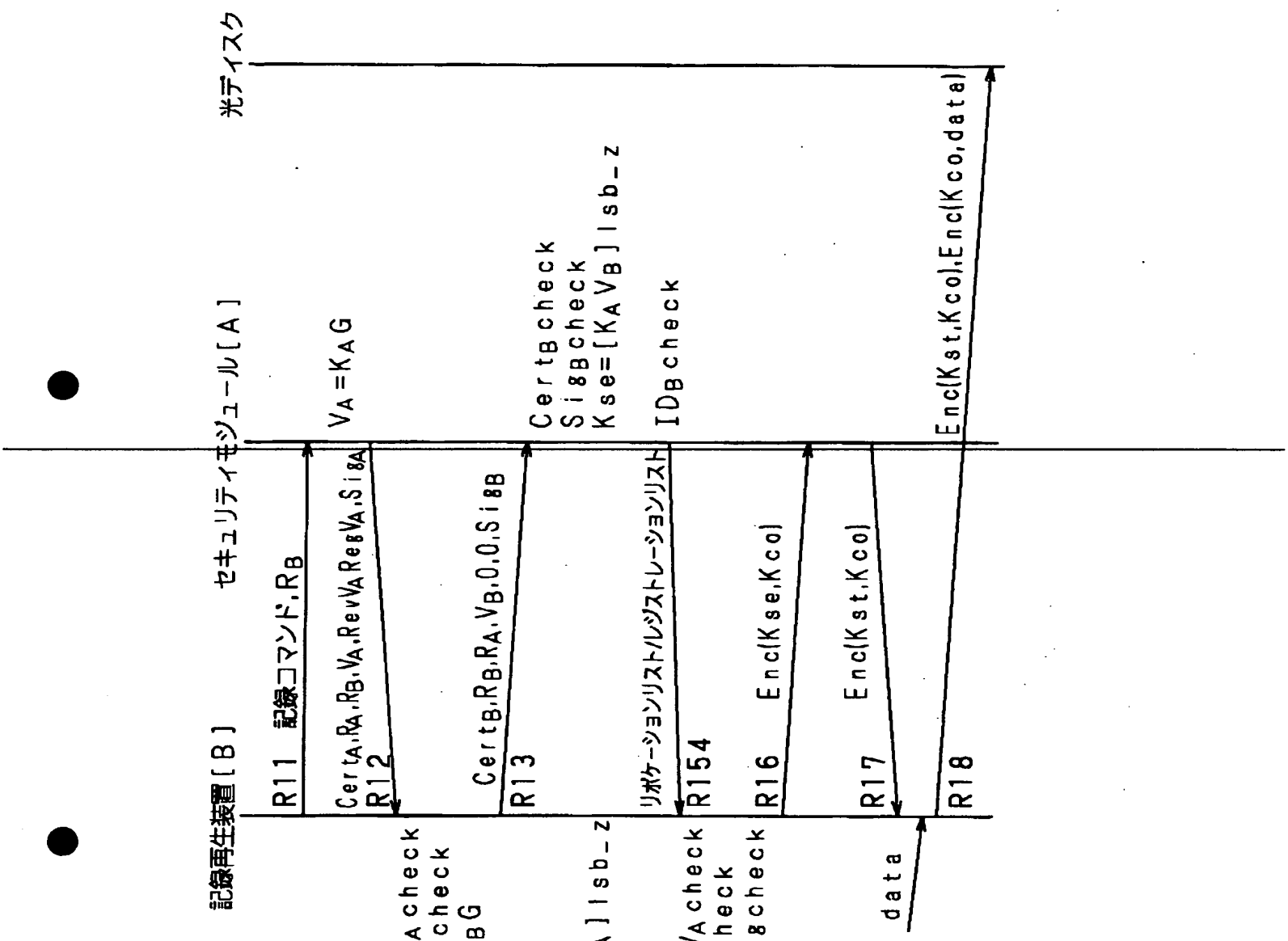
【図６５】


300
104
104A
暗号化部
104B
復号部
記録／再生回路
記録信号
再生信号
107
乱数発生部
109
演算部
105
制御部
106
入力部
ピックアップ
102
サーボ回路
103
スピンドルモータ
101
10
11
12
13
108

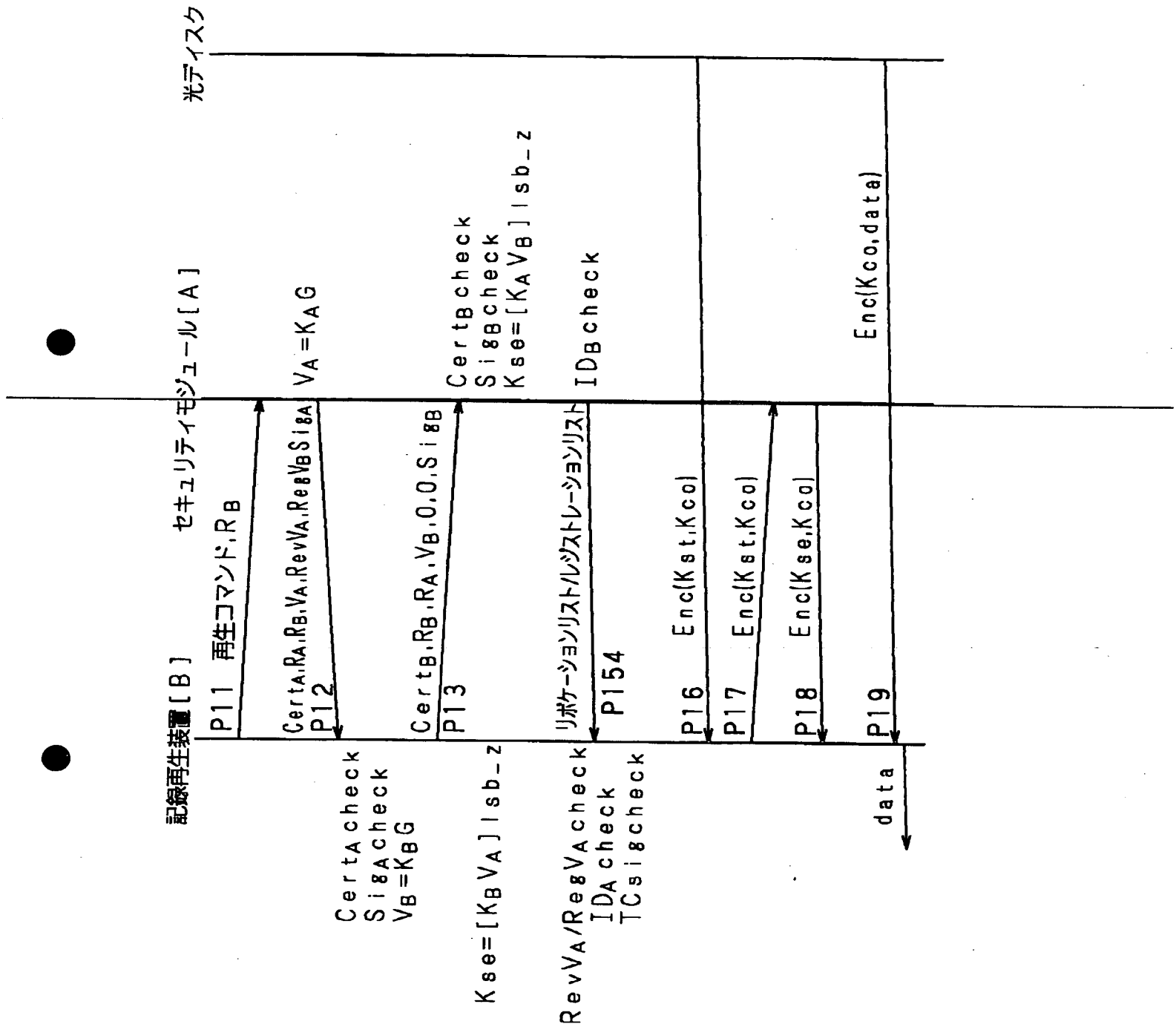
【図６６】


ＩＤ
秘密鍵
公開鍵
公開鍵証明書
ＩＤ
秘密鍵
公開鍵
公開鍵証明書
リボケーションリスト／
レジストレーションリスト
記録再生装置
セキュリティモジュール
光ディスク
記録コマンド
R1 Recording-ID
相互認証(リスト検査除く)
Ｋｓｅ共有
R2 バージョンナンバー
リボケーションリスト/
レジストレーションリスト
R143
data
R5 Enc(Kco,data)
Enc(Kco,data)

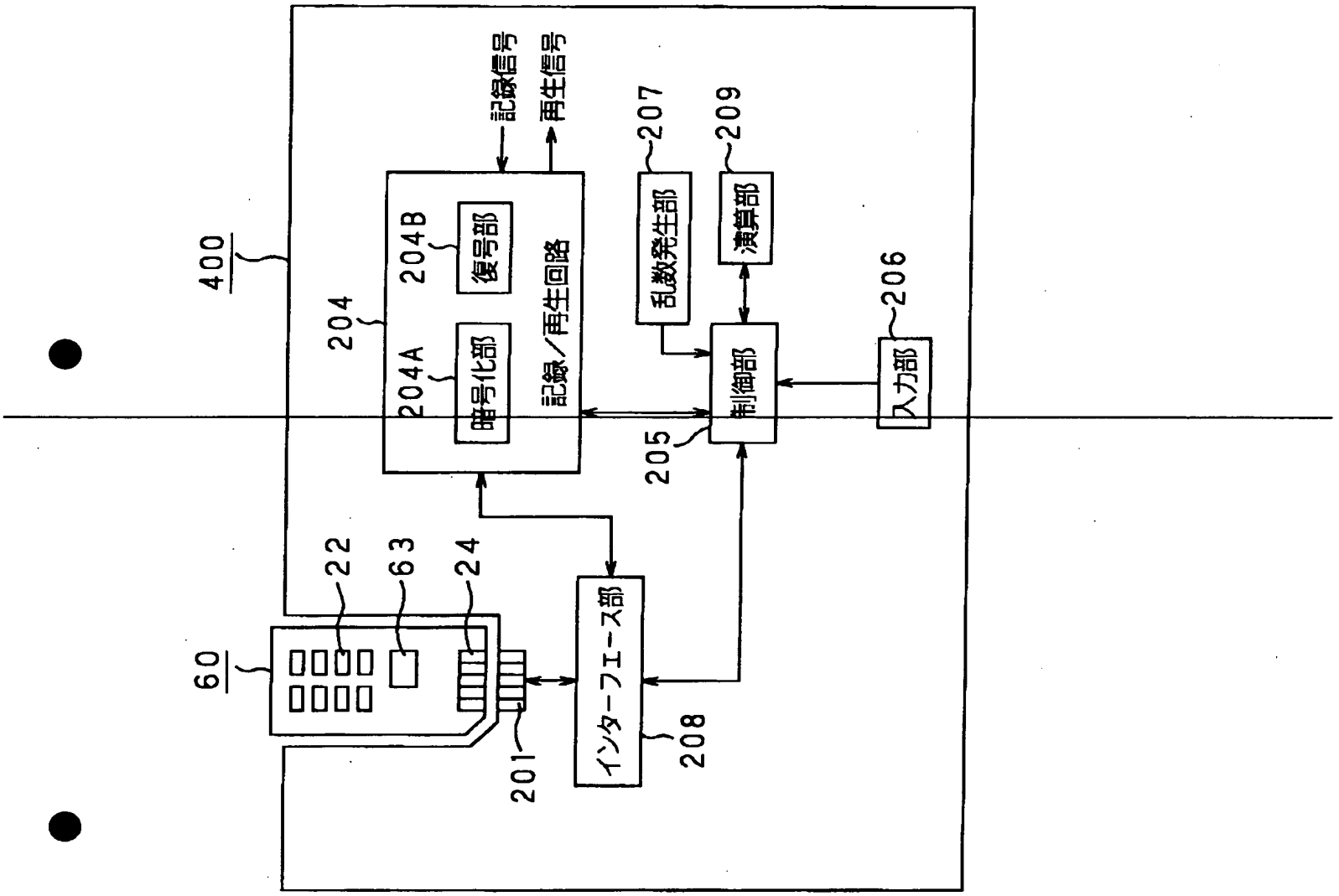
【図６７】


光ディスク
セキュリティモジュール[A]
記録再生装置[B]
R11 記録コマンド,RB
VA=KAG
CertA,RA,RB,VA,RevVA,RegVA,SigA
R12
CertA check
SigA check
VB=KBG
CertB,RB,RA,VB,0,0,SigB
R13
CertB check
SigB check
Kse=[KAVB]lsb_z
Kse=[KBVA]lsb_z
IDB check
リボケーションリストレジストレーションリスト
R154
RevVA/RegVA check
IDA check
TCsigcheck
R16 Enc(Kse,Kcol)
R17 Enc(Kst,Kcol)
data
R18 Enc(Kst,Kco),Enc(Kco,data)

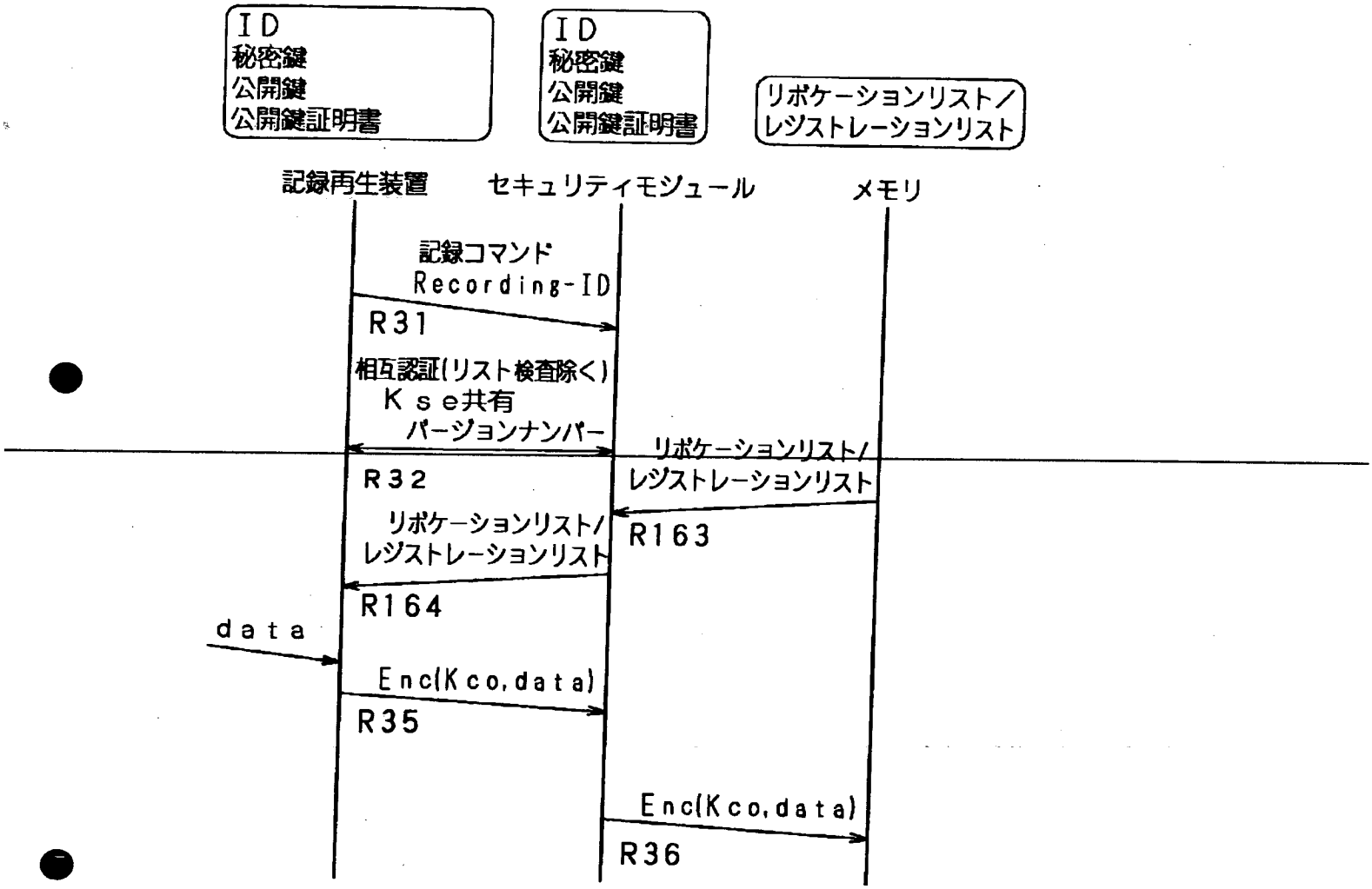
【図６８】


記録再生装置[B]
セキュリティモジュール[A]
光ディスク
P11 再生コマンド,RB
CertA,RA,RB,VA,RevVA,RegVB,SigA
P12
CertB,RB,RA,VB,0,0,SigB
P13
リボケーションリストレジストレーションリスト
P154
P16 Enc(Kst,Kcol)
P17 Enc(Kst,Kcol)
P18 Enc(Kse,Kcol)
P19
data
VA=KAG
CertB check
SigB check
Kse=[KAVB]lsb_z
IDB check
Enc(Kco,data)
CertA check
SigA check
VB=KBG
Kse=[KBVA]lsb_z
RevVA/RegVA check
IDA check
TCsig check

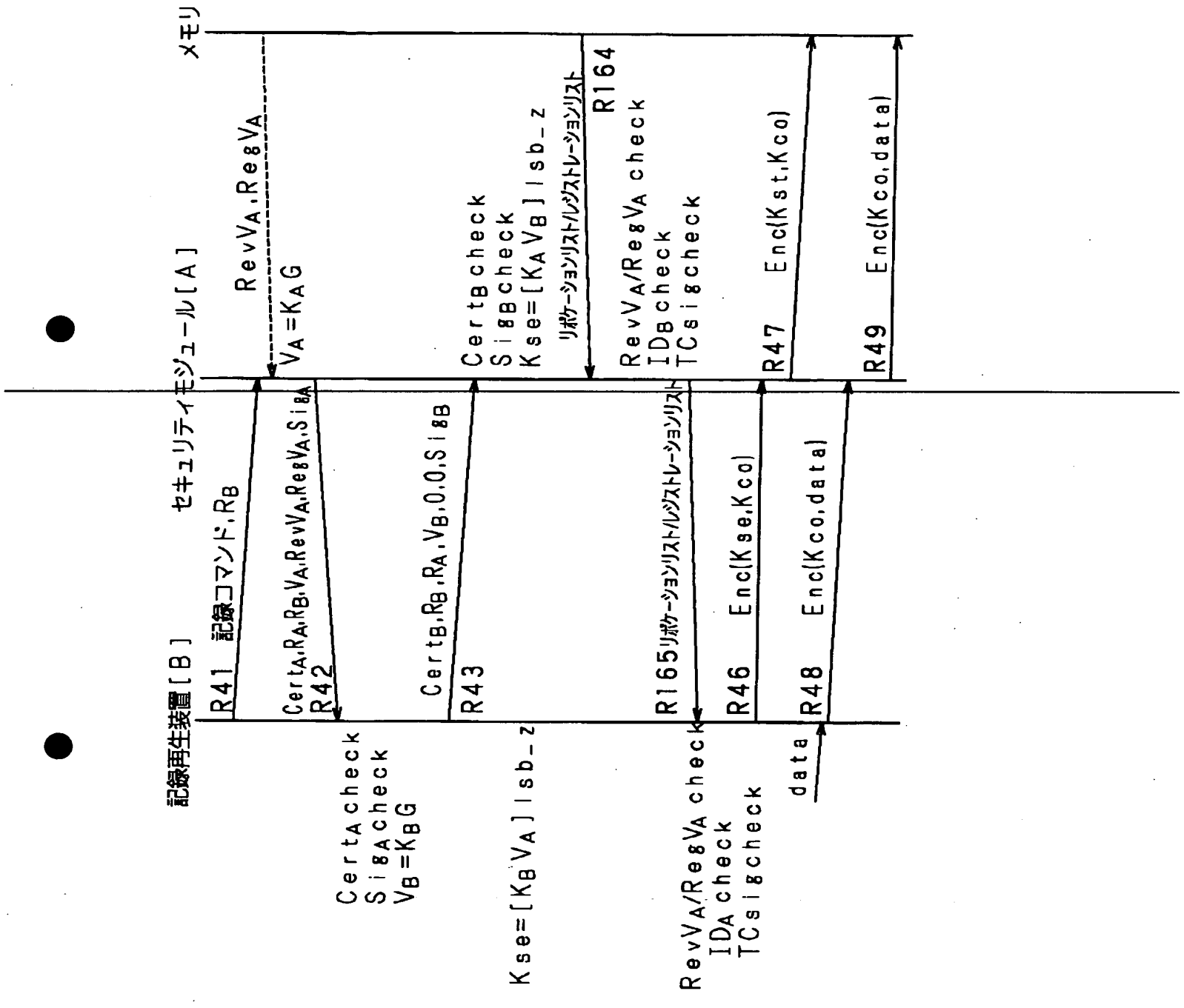
【図６９】


400
204
204A
暗号化部
204B
復号部
記録／再生回路
記録信号
再生信号
207
乱数発生部
209
演算部
206
入力部
制御部
205
60
22
63
24
インターフェース部
201
208

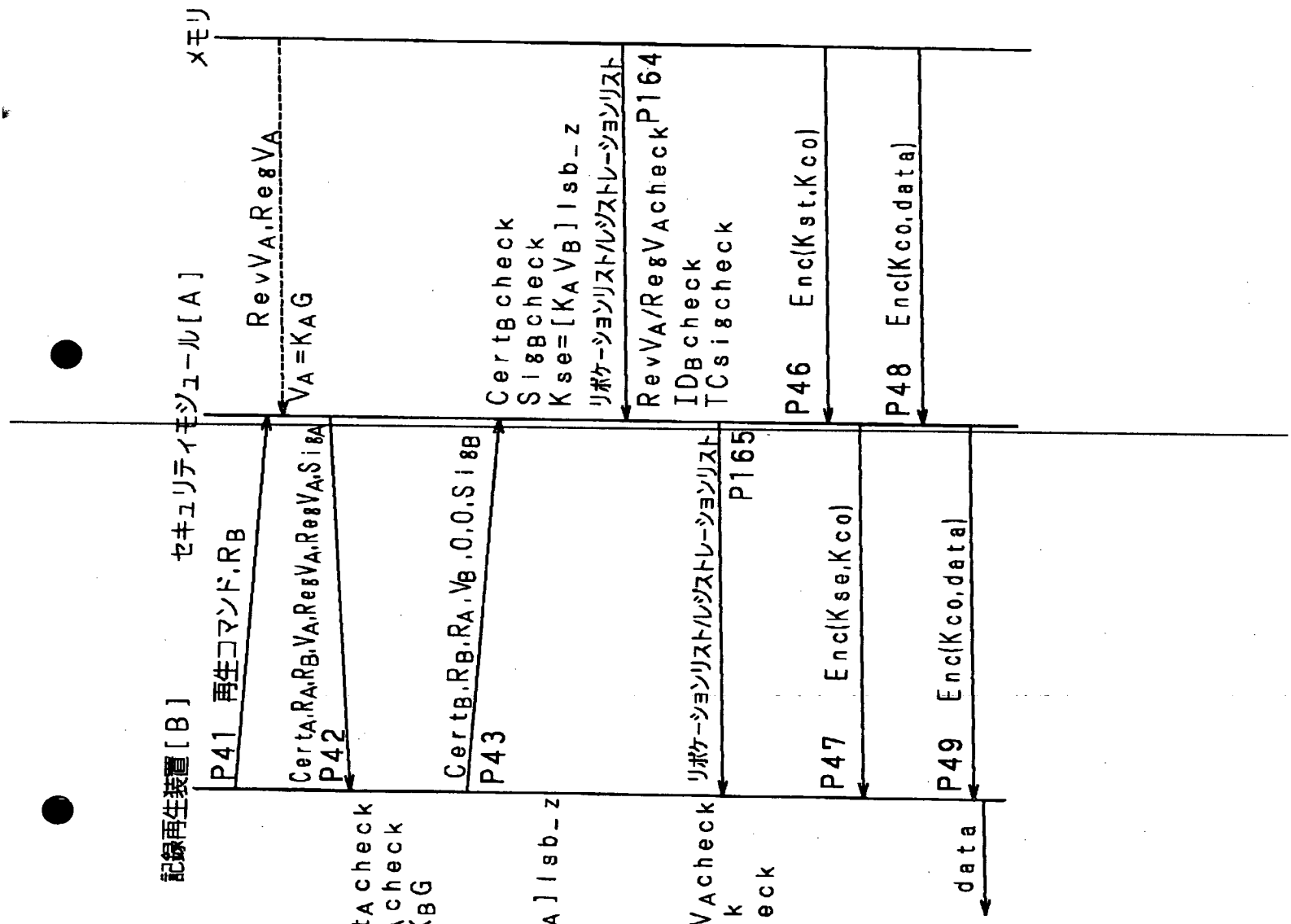
【図７０】


ＩＤ
秘密鍵
公開鍵
公開鍵証明書
ＩＤ
秘密鍵
公開鍵
公開鍵証明書
リボケーションリスト／
レジストレーションリスト
記録再生装置
セキュリティモジュール
メモリ
記録コマンド
Ｒｅｃｏｒｄｉｎｇ－ＩＤ
Ｒ３１
相互認証(リスト検査除く)
Ｋｓｅ共有
バージョンナンバー
Ｒ３２
リボケーションリスト／
レジストレーションリスト
Ｒ１６３
リボケーションリスト／
レジストレーションリスト
Ｒ１６４
ｄａｔａ
Ｅｎｃ(Ｋｃｏ,ｄａｔａ)
Ｒ３５
Ｅｎｃ(Ｋｃｏ,ｄａｔａ)
Ｒ３６

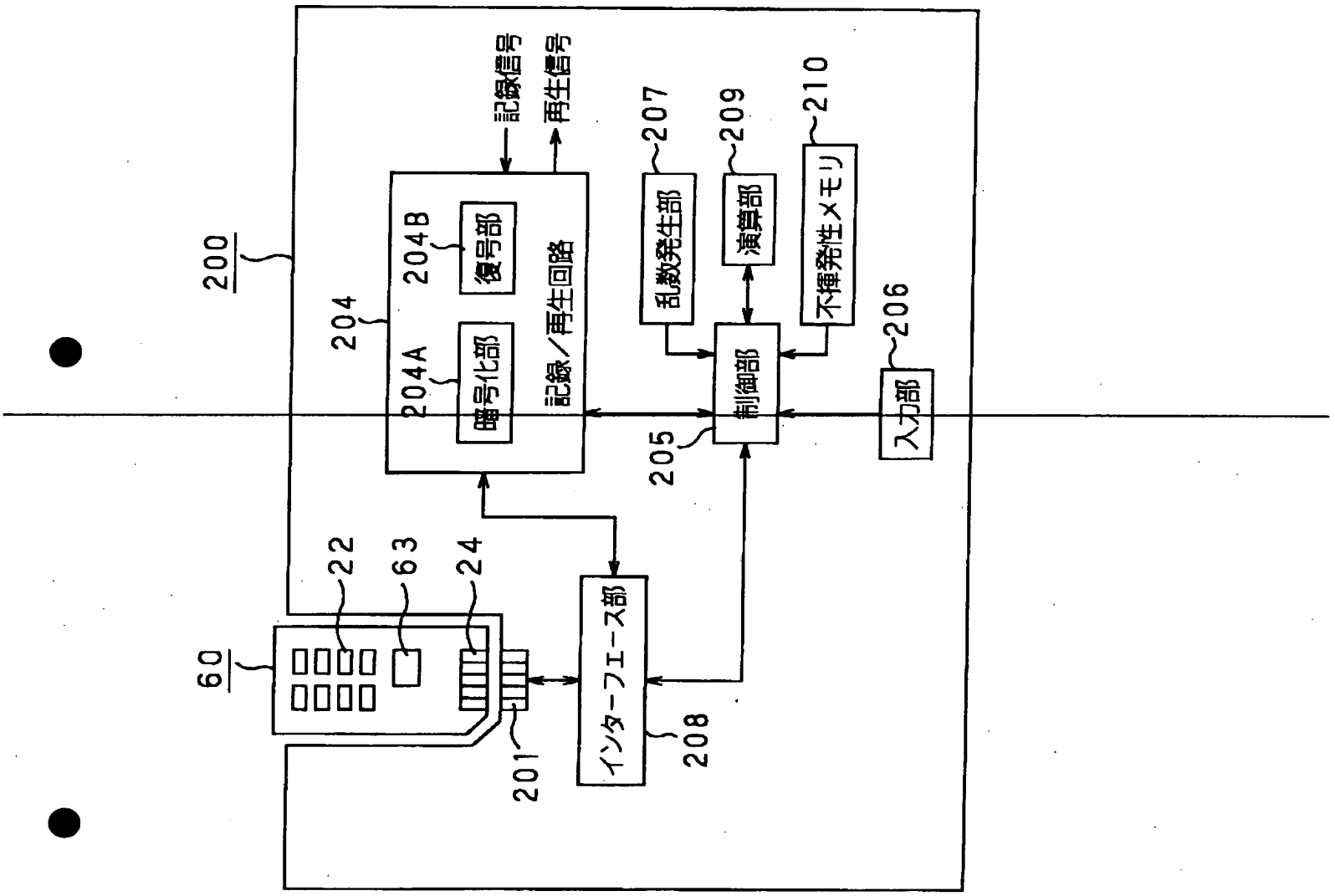
【図７１】


メモリ
セキュリティモジュール[A]
記録再生装置[B]
RevVA,RegVA
VA=KAG
R41 記録コマンド,RB
CertA,RA,RB,VA,RevVA,RegVA,SigA
R42
CertB,RB,RA,VB,0,0,SigB
R43
R164
CertB check
SigB check
Kse=[KA VB] Isb_z
リボケーションリストレジストレーションリスト
RevVA/RegVA check
IDB check
TCsig check
R165 リボケーションリストレジストレーションリスト
R46 Enc(Kse,Kco)
R47 Enc(Kst,Kco)
R48 Enc(Kco,data)
R49 Enc(Kco,data)
CertA check
SigA check
VB=KBG
Kse=[KB VA] Isb_z
RevVA/RegVA check
IDA check
TCsig check
data

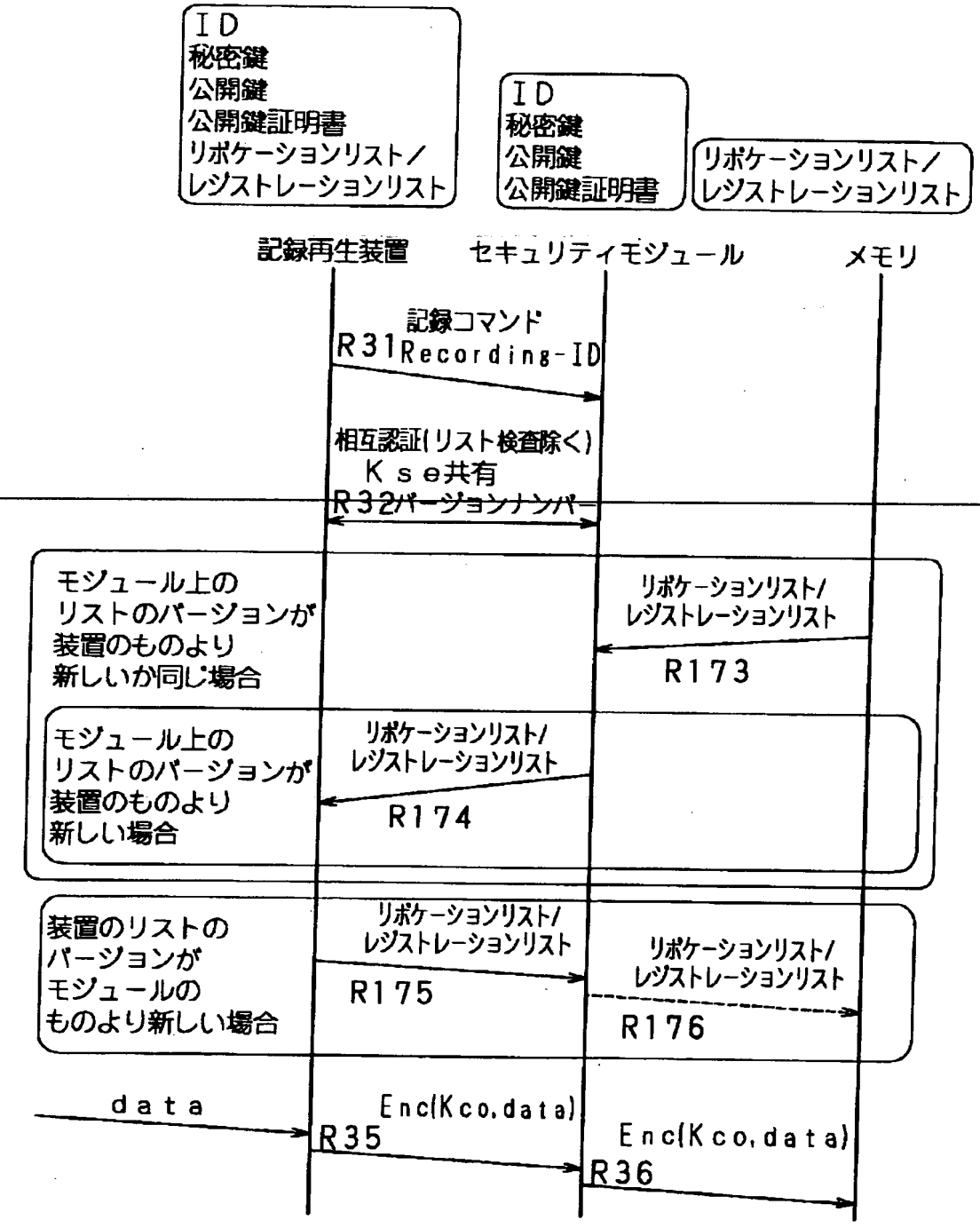
【図７２】


メモリ
セキュリティモジュール[A]
記録再生装置[B]
RevVA,RegVA
VA=KAG
CertB check
SigB check
Kse=[KAVB]Isb_z
リボケーションリスト/リジストレーションリスト
RevVA/RegVA check P164
IDB check
TCsig check
P46 Enc(Kst,Kco)
P48 Enc(Kco,data)
P41 再生コマンド,RB
CertA,RA,RB,VA,RegVA,RegVA,SigA P42
CertB,RB,RA,VB,0,0,SigB P43
リボケーションリスト/リジストレーションリスト P165
P47 Enc(Kse,Kco)
P49 Enc(Kco,data)
CertA check
SigA check
VB=KBG
Kse=[KBVA]Isb_z
RevVA/RegVA check
IDA check
TCsig check
data

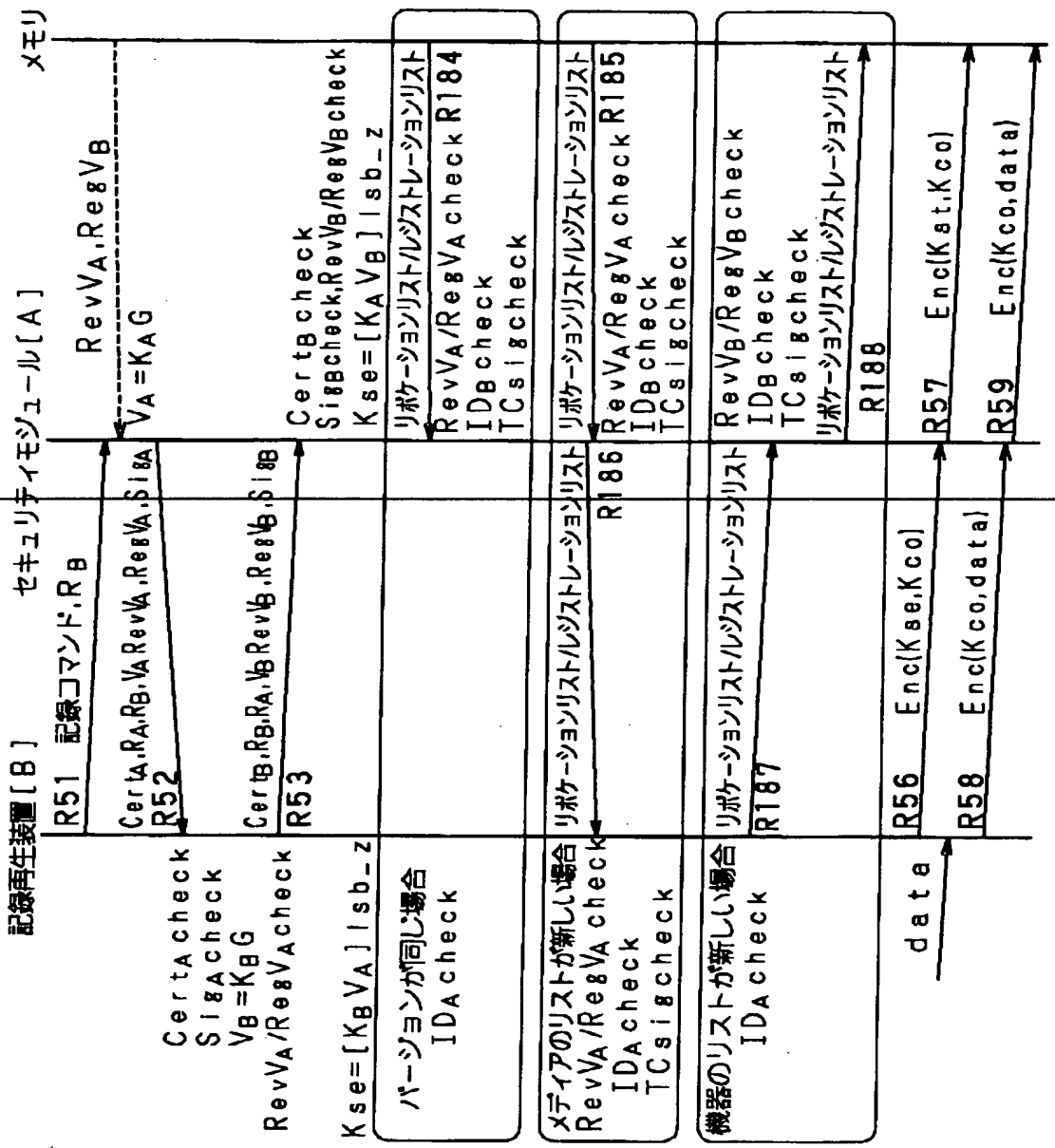
【図７３】


200
記録信号
再生信号
204
204B
復号部
204A
暗号化部
記録／再生回路
207
乱数発生部
209
演算部
210
不揮発性メモリ
206
入力部
制御部
205
22
63
24
60
インターフェース部
208
201

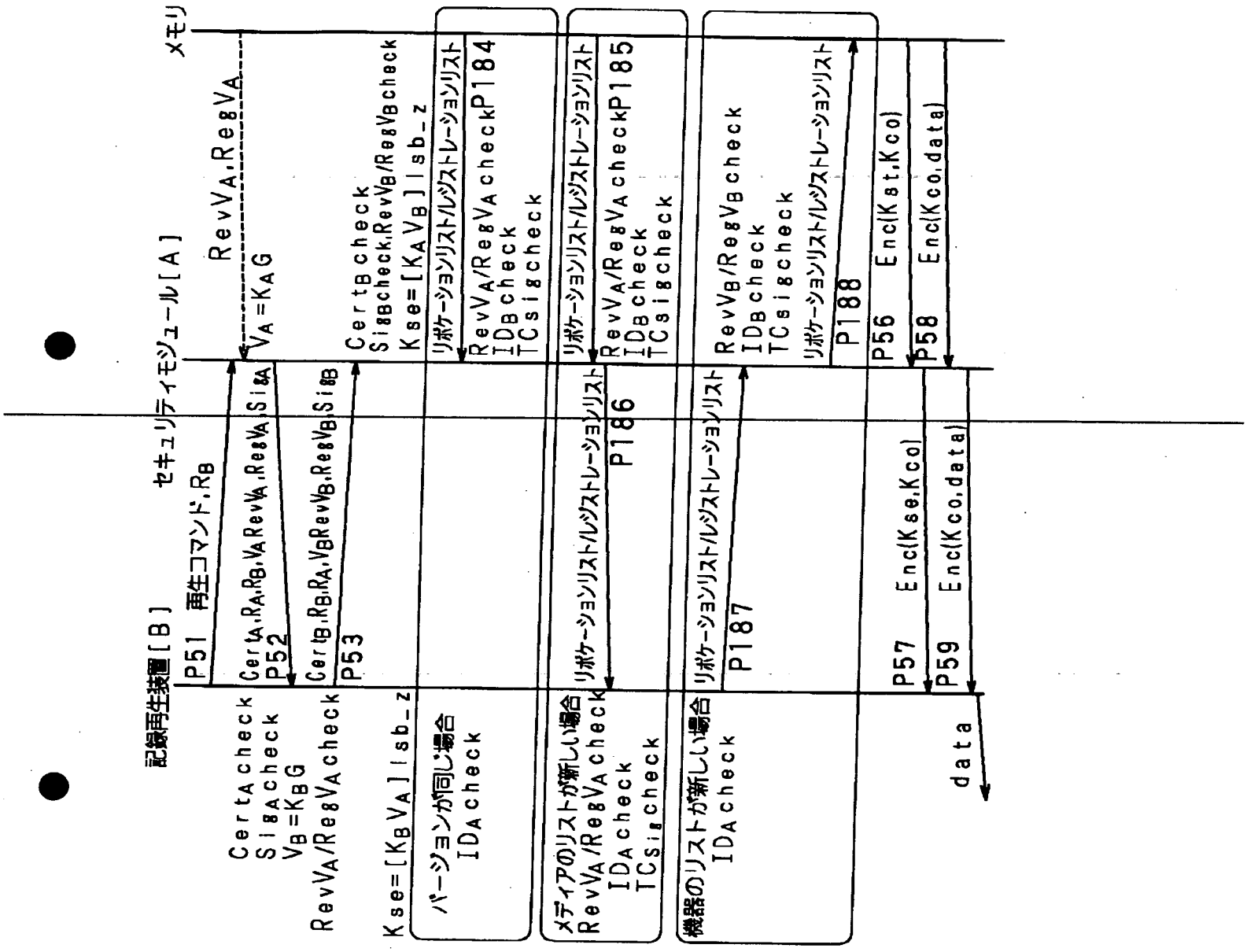
【図７４】


ＩＤ
秘密鍵
公開鍵
公開鍵証明書
リポケーションリスト／
レジストレーションリスト
ＩＤ
秘密鍵
公開鍵
公開鍵証明書
リポケーションリスト／
レジストレーションリスト
記録再生装置
セキュリティモジュール
メモリ
記録コマンド
R31Recording-ID
相互認証(リスト検査除く)
Ｋｓｅ共有
R32バージョンナンバー
モジュール上の
リストのバージョンが
装置のものより
新しいか同じ場合
リポケーションリスト/
レジストレーションリスト
R173
モジュール上の
リストのバージョンが
装置のものより
新しい場合
リポケーションリスト/
レジストレーションリスト
R174
装置のリストの
バージョンが
モジュールの
ものより新しい場合
リポケーションリスト/
レジストレーションリスト
R175
リポケーションリスト/
レジストレーションリスト
R176
ｄａｔａ
Enc(Kco,data)
R35
Enc(Kco,data)
R36

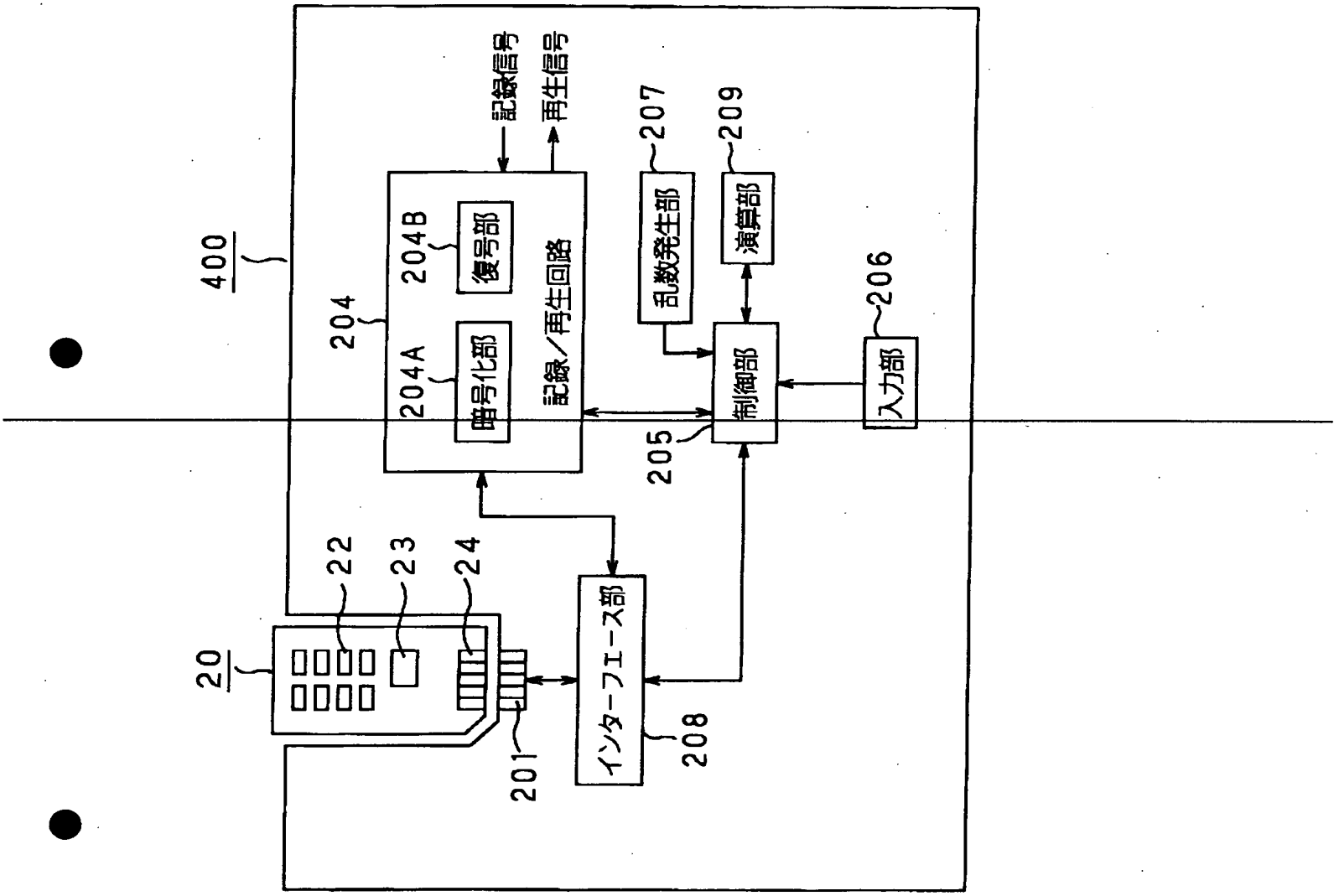
【図７５】


記録再生装置[B]
セキュリティモジュール[A]
メモリ
R51 記録コマンド,RB
RevVA,RegVB
VA=KAG
CertA,RA,RB,VA RevVA,RegVA,SigA
R52
CertB,RB,RA,VB RevVB,RegVB,SigB
R53
CertB check
SigBcheck,RevVB/RegVBcheck
Kse=[KA VB]Isb_z
リボケーションリスト/リジストレーションリスト
RevVA/RegVA check R184
IDB check
TCsigcheck
リボケーションリスト/リジストレーションリスト
R186
リボケーションリスト/リジストレーションリスト
RevVA/RegVA check R185
IDB check
TCsigcheck
リボケーションリスト/リジストレーションリスト
R187
RevVB/RegVB check
IDB check
TCsigcheck
リボケーションリスト/リジストレーションリスト
R188
R56 Enc(Kse,Kcol)
R57 Enc(Kst,Kcol)
R58 Enc(Kco,data)
R59 Enc(Kco,data)
CertA check
SigA check
VB=KBG
RevVA/RegVA check
Kse=[KB VA]Isb_z
バージョンが同じ場合
IDA check
メディアのリストが新しい場合
RevVA/RegVA check
IDA check
TCsigcheck
機器のリストが新しい場合
IDA check
data

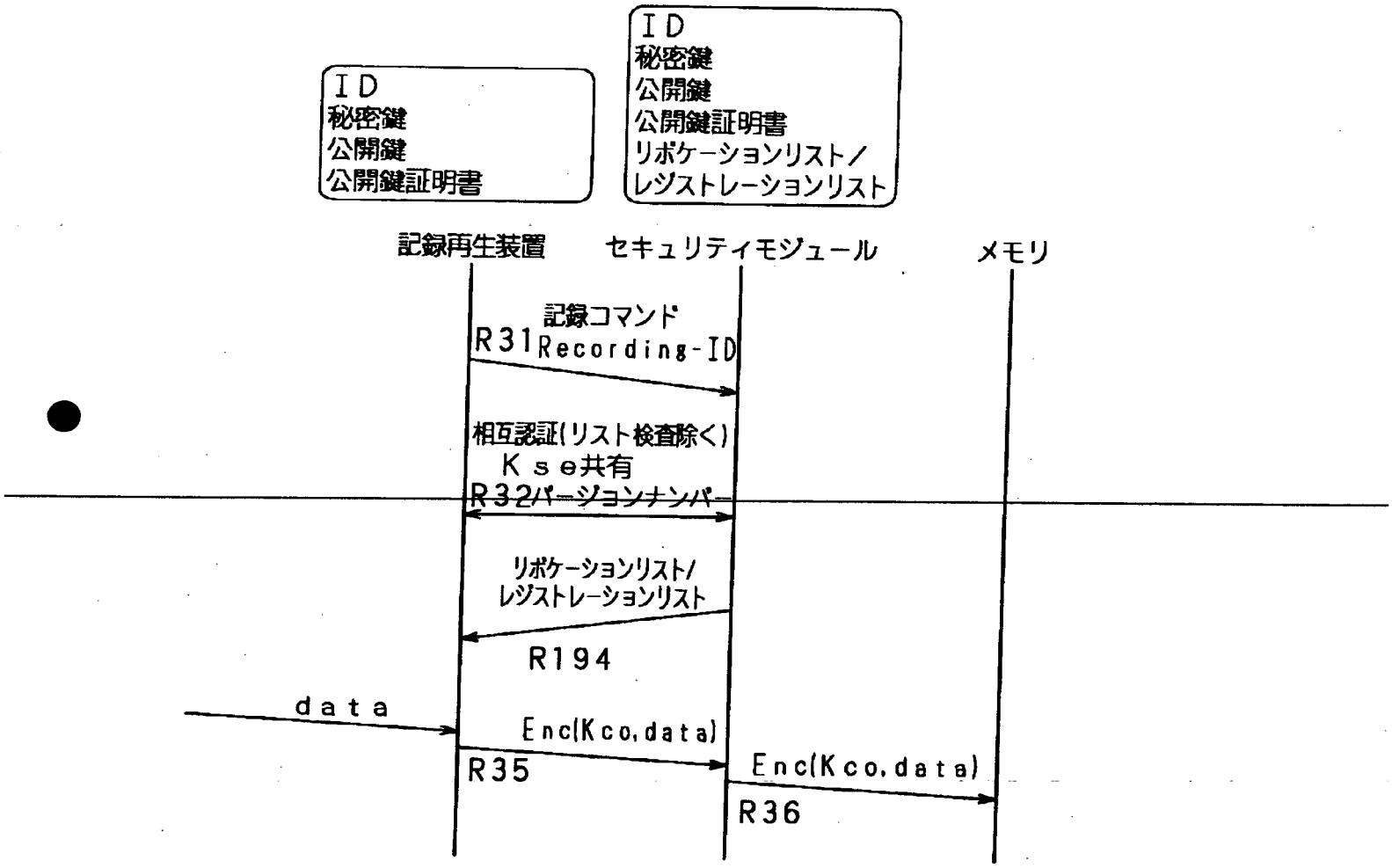
【図７６】


記録再生装置[B]
セキュリティモジュール[A]
メモリ
P51 再生コマンド,RB
CertA,RA,RB,VA RevVA,RegVA,SigA
P52
CertB,RB,RA,VB RevVB,RegVB,SigB
P53
RevVA,RegVA
VA=KAG
CertB check
SigBcheck,RevVB/RegVBcheck
Kse=[KAVB]Isb_z
リボケーションリスト/リジストレーションリスト
RevVA/RegVA checkP184
IDB check
TCsig check
リボケーションリスト/リジストレーションリスト
RevVA/RegVA checkP185
IDB check
TCsig check
リボケーションリスト/リジストレーションリスト
RevVB/RegVB check
IDB check
TCsig check
リボケーションリスト/リジストレーションリスト
P188
P56 Enc(Kst,Kco)
P58 Enc(Kco,data)
CertA check
SigA check
VB=KBG
RevVA/RegVA check
Kse=[KBVA]Isb_z
バージョンが同じ場合
IDA check
メディアのリストが新しい場合
RevVA/RegVA check
IDA check
TCsig check
リボケーションリスト/リジストレーション
P186
機器のリストが新しい場合
IDA check
リボケーションリスト/リジストレーション
P187
P57 Enc(Kse,Kco)
P59 Enc(Kco,data)
data

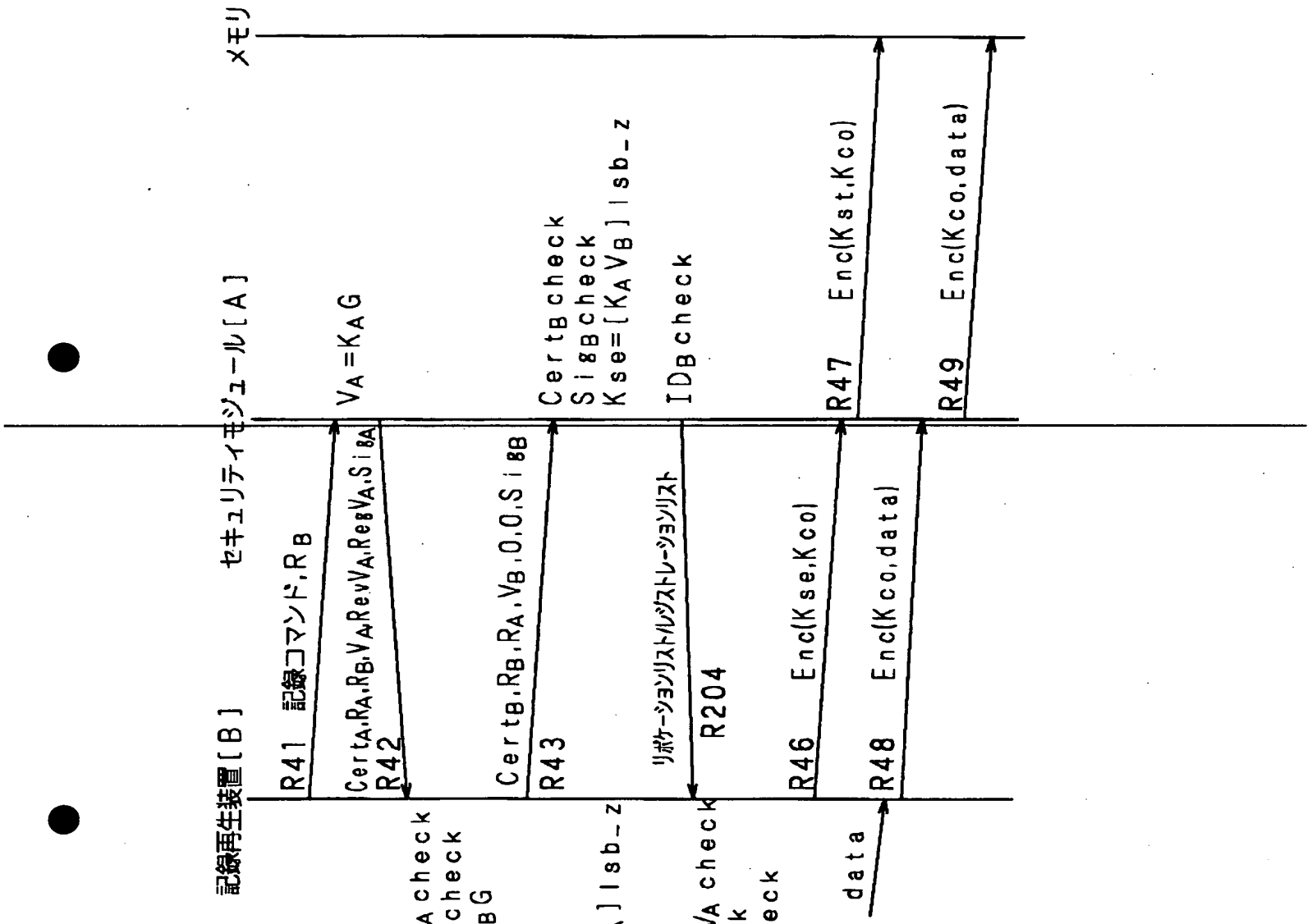
【図７７】


400
記録信号
再生信号
204
204B
復号部
204A
暗号化部
記録／再生回路
207
乱数発生部
209
演算部
206
入力部
制御部
205
22
23
24
20
インターフェース部
201
208

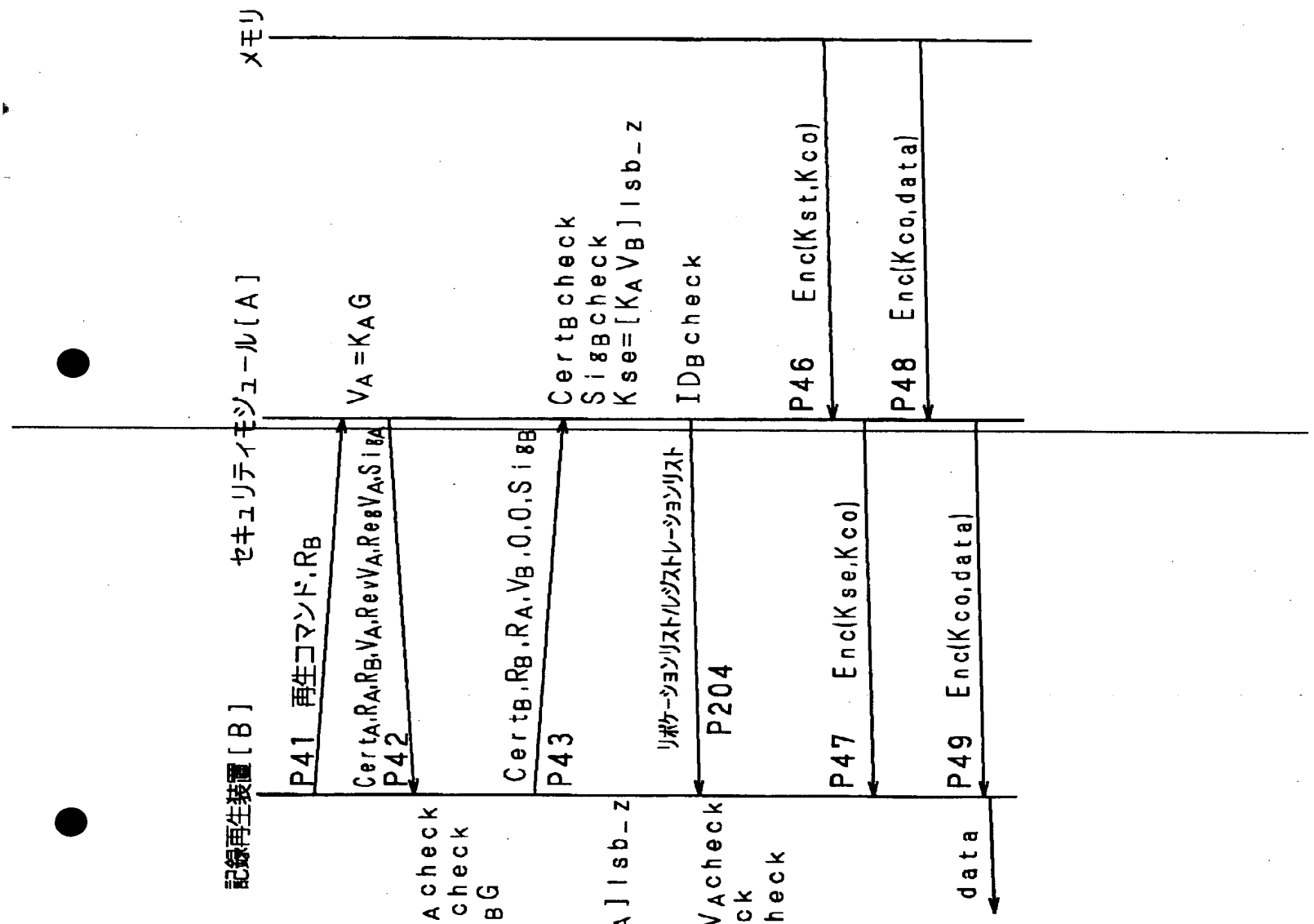
【図７８】


ＩＤ
秘密鍵
公開鍵
公開鍵証明書
ＩＤ
秘密鍵
公開鍵
公開鍵証明書
リボケーションリスト／
レジストレーションリスト
記録再生装置
セキュリティモジュール
メモリ
記録コマンド
R31 Recording-ID
相互認証(リスト検査除く)
Ｋｓｅ共有
R32 バージョンナンバー
リボケーションリスト/
レジストレーションリスト
R194
data
Enc(Kco,data)
R35
Enc(Kco,data)
R36

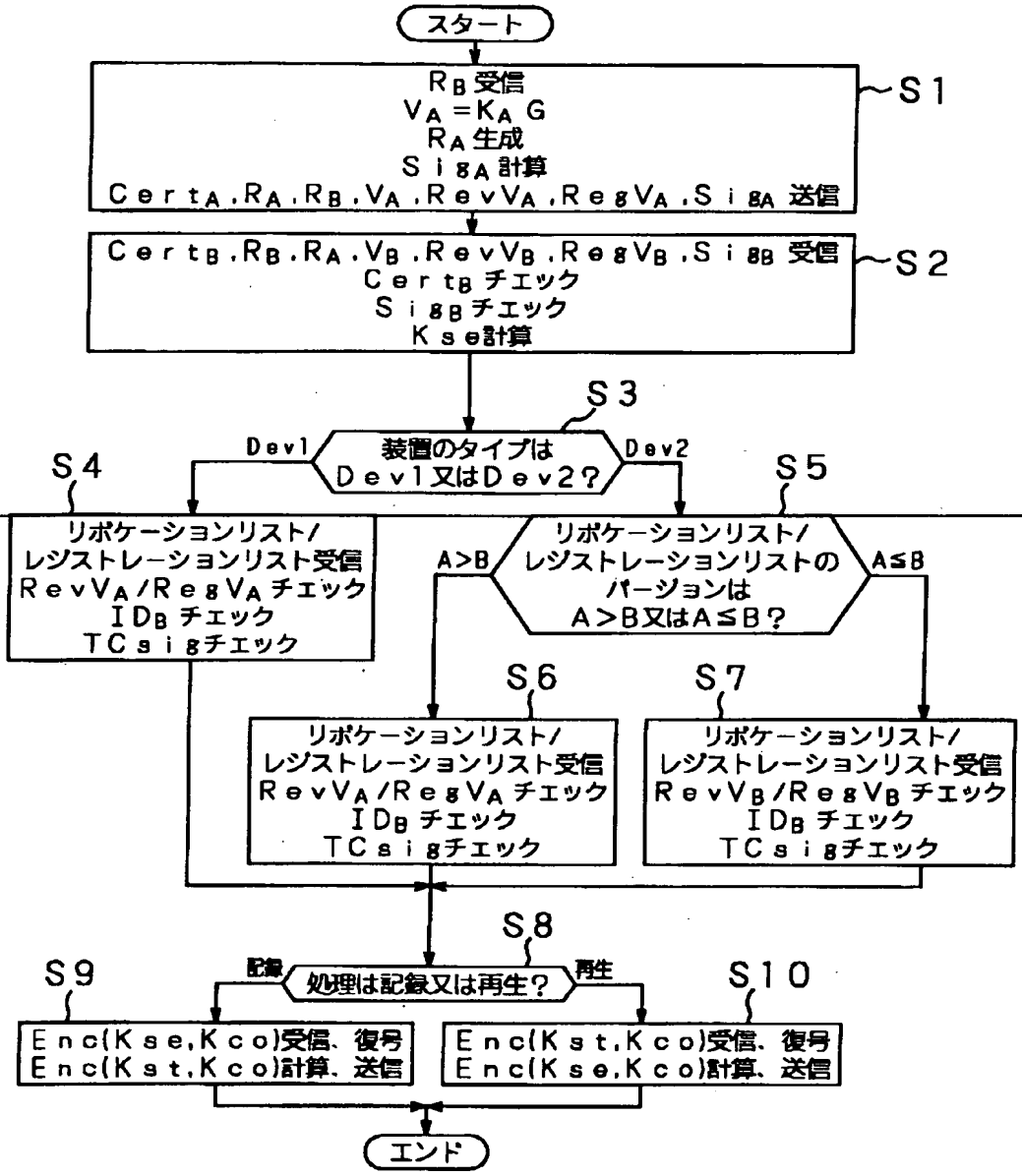
【図７９】


メモリ
セキュリティモジュール[A]
記録再生装置[B]
記録コマンド,RB
R41
CertA,RA,RB,VA,RevVA,RegVA,SigA
R42
CertB,RB,RA,VB,0,0,SigB
R43
リボケーションリスト,バックストレーションリスト
R204
R46
Enc(Kse,Kcol)
R48
Enc(Kco,data)
R47
Enc(Kst,Kco)
R49
Enc(Kco,data)
VA=KAG
CertA check
SigA check
VB=KBG
Kse=[KBVA]Isb_z
CertB check
SigB check
Kse=[KAVB]Isb_z
IDB check
RevVA/RegVA check
IDA check
TCsig check
data

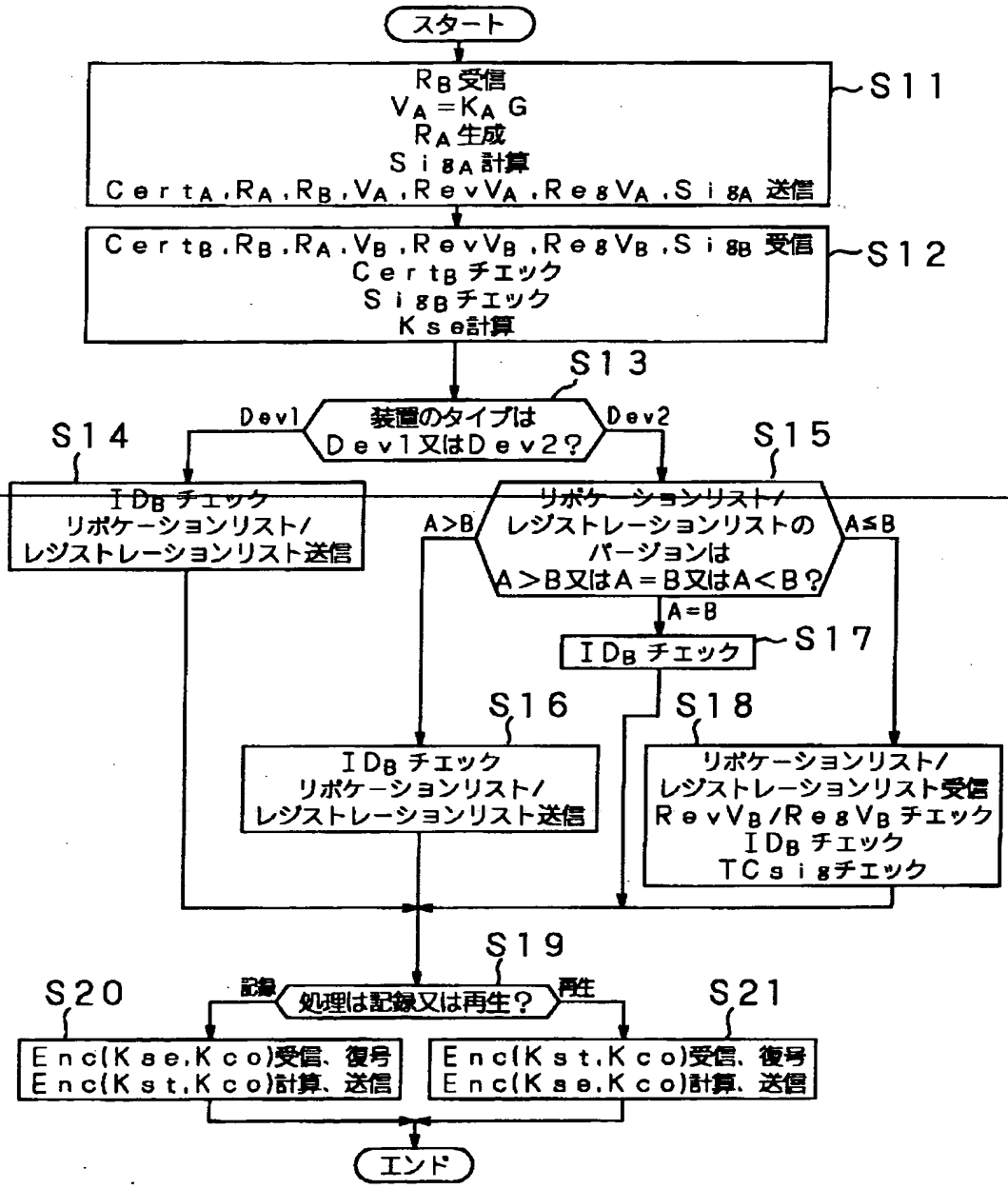
【図８０】


メモリ
セキュリティモジュール[A]
記録再生装置[B]
P41 再生コマンド,RB
CertA,RA,RB,VA,RevVA,RegVA,SigA
P42
CertA check
SigA check
VB=KBG
CertB,RB,RA,VB,0,0,SigB
P43
Kse=[KBVA]Isb_z
リボケーションリストバリストレーションリスト
P204
RevVA/RegVA check
IDA check
TCsig check
VA=KAG
CertB check
SigB check
Kse=[KAVB]Isb_z
IDB check
P46 Enc(Kst,Kco)
P47 Enc(Kse,Kco)
P48 Enc(Kco,data)
P49 Enc(Kco,data)
data

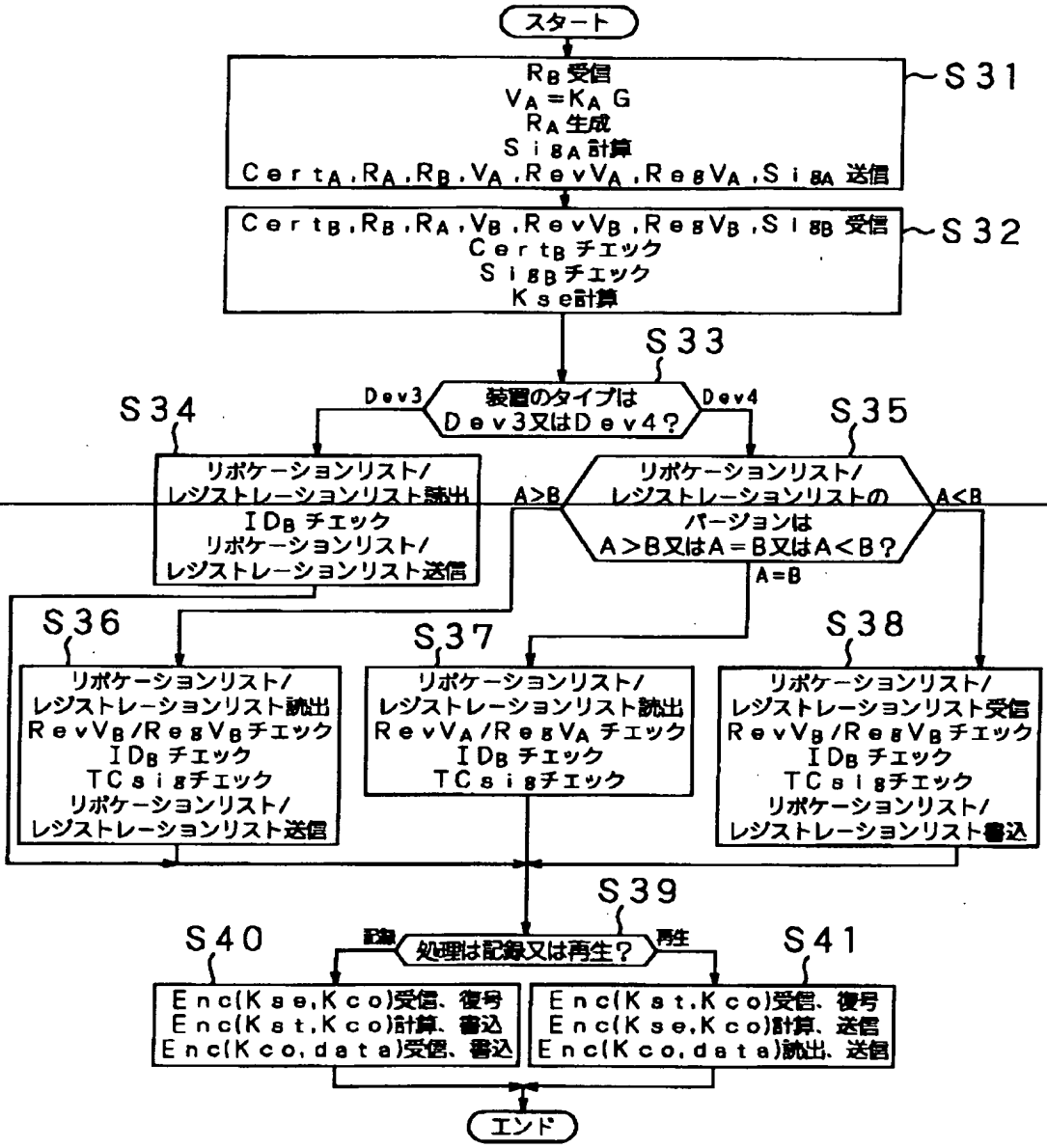
【図８１】


スタート
R_B受信
$V_A = K_A G$
R_A生成
Sig_A計算
$Cert_A, R_A, R_B, V_A, RevV_A, RegV_A, Sig_A$送信
S1
$Cert_B, R_B, R_A, V_B, RevV_B, RegV_B, Sig_B$受信
$Cert_B$チェック
Sig_Bチェック
Kse計算
S2
S3
装置のタイプは
Dev1又はDev2？
Dev1
Dev2
S4
リポケーションリスト/
レジストレーションリスト受信
$RevV_A/RegV_A$チェック
ID_Bチェック
TCsigチェック
S5
リポケーションリスト/
レジストレーションリストの
バージョンは
A>B又はA≦B？
A>B
A≦B
S6
リポケーションリスト/
レジストレーションリスト受信
$RevV_A/RegV_A$チェック
ID_Bチェック
TCsigチェック
S7
リポケーションリスト/
レジストレーションリスト受信
$RevV_B/RegV_B$チェック
ID_Bチェック
TCsigチェック
S8
処理は記録又は再生？
記録
再生
S9
Enc(Kse,Kco)受信、復号
Enc(Kst,Kco)計算、送信
S10
Enc(Kst,Kco)受信、復号
Enc(Kse,Kco)計算、送信
エンド

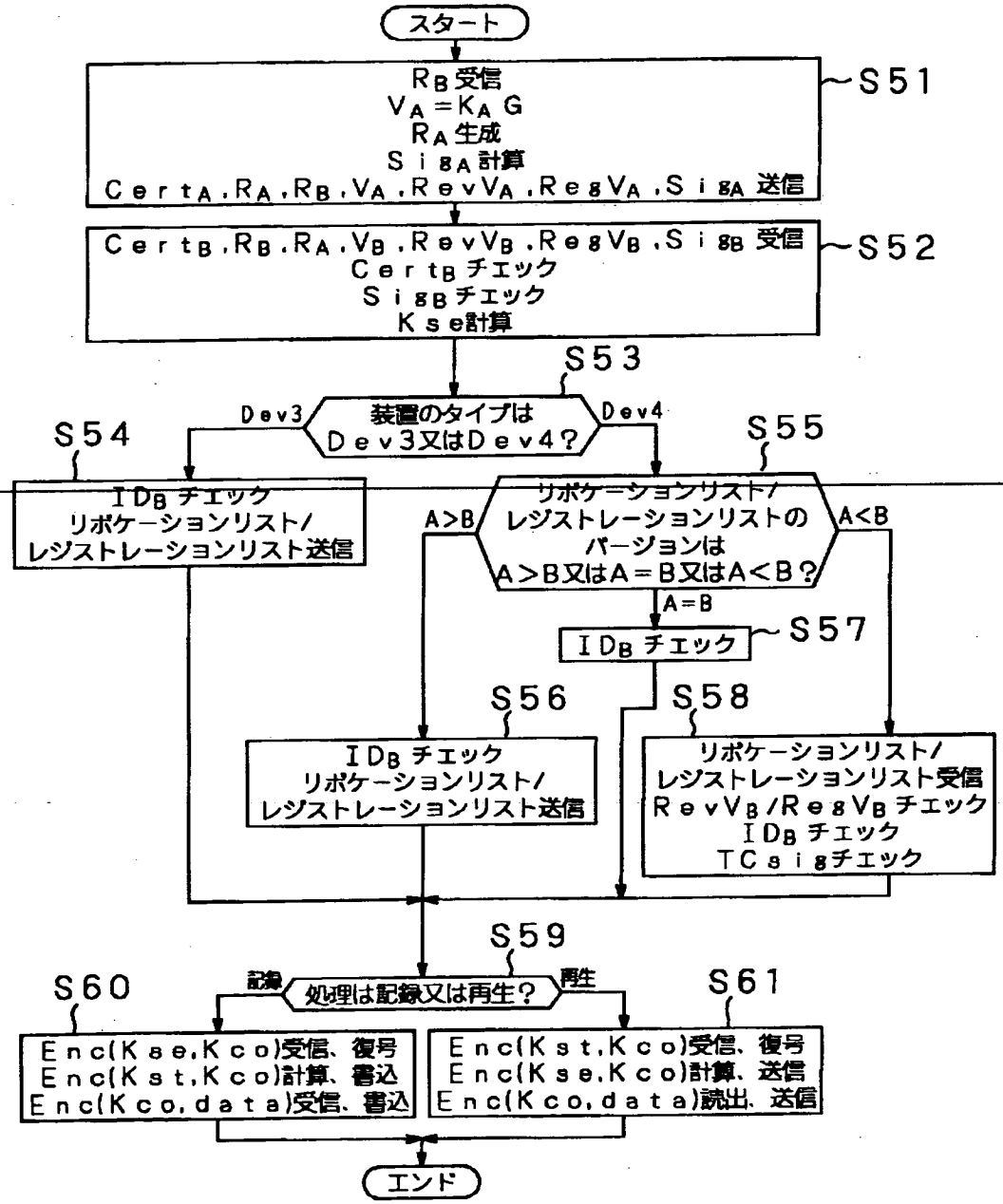
【図８２】


スタート
R_B受信
$V_A = K_A G$
R_A生成
Sig_A計算
$Cert_A, R_A, R_B, V_A, RevV_A, RegV_A, Sig_A$送信
S11
$Cert_B, R_B, R_A, V_B, RevV_B, RegV_B, Sig_B$受信
$Cert_B$チェック
Sig_Bチェック
Kse計算
S12
S13
装置のタイプは
Dev1又はDev2？
Dev1
Dev2
S14
ID_Bチェック
リポケーションリスト/
レジストレーションリスト送信
S15
リポケーションリスト/
レジストレーションリストの
バージョンは
A＞B又はA＝B又はA＜B？
A>B
A≦B
A=B
ID_Bチェック
S17
S16
ID_Bチェック
リポケーションリスト/
レジストレーションリスト送信
S18
リポケーションリスト/
レジストレーションリスト受信
$RevV_B$/$RegV_B$チェック
ID_Bチェック
TCsigチェック
S19
処理は記録又は再生？
記録
再生
S20
Enc(Kse,Kco)受信、復号
Enc(Kst,Kco)計算、送信
S21
Enc(Kst,Kco)受信、復号
Enc(Kse,Kco)計算、送信
エンド

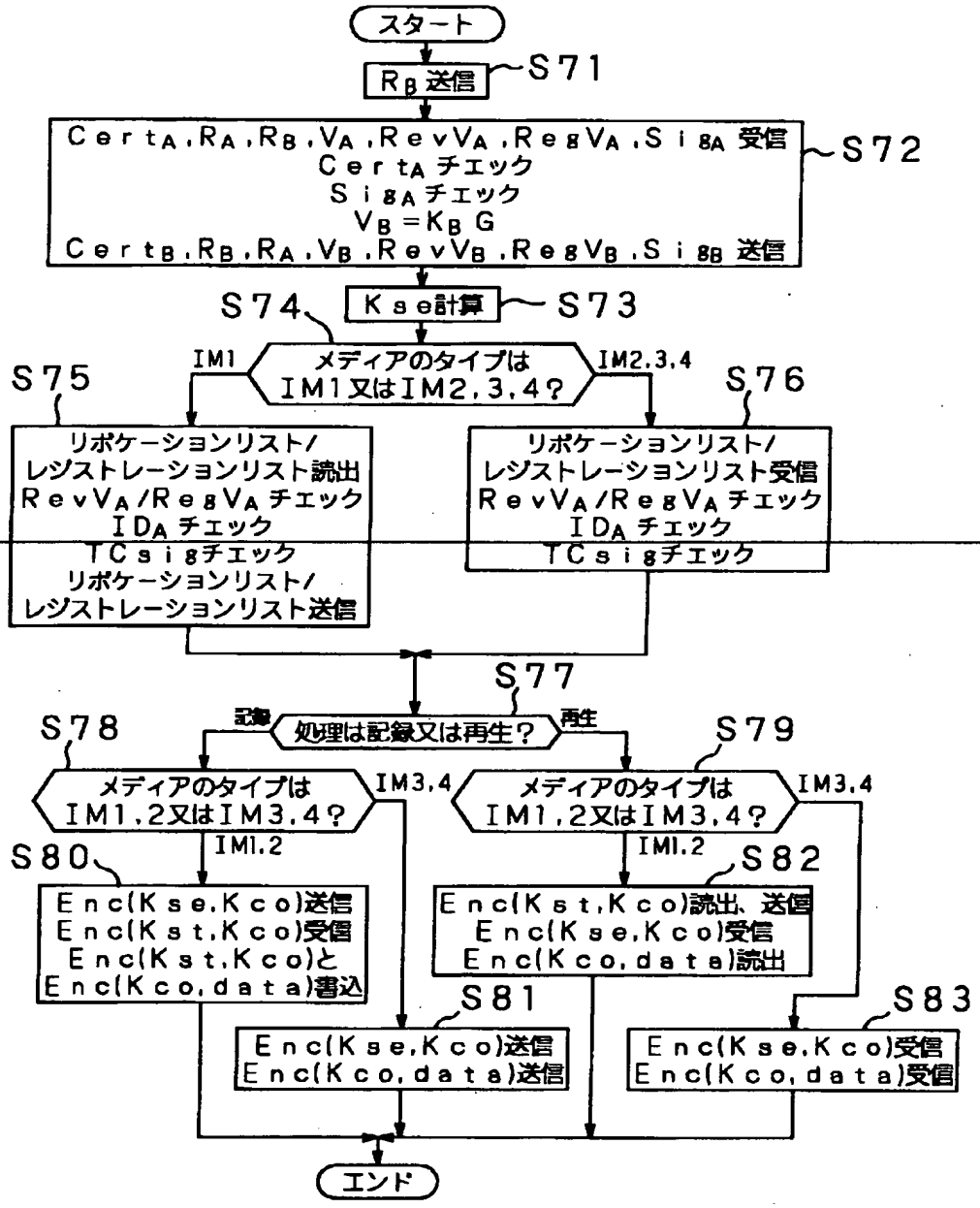
【図８３】


スタート
R_B受信
$V_A=K_A G$
R_A生成
Sig_A計算
$Cert_A, R_A, R_B, V_A, RevV_A, RegV_A, Sig_A$送信
S31
$Cert_B, R_B, R_A, V_B, RevV_B, RegV_B, Sig_B$受信
$Cert_B$チェック
Sig_Bチェック
Kse計算
S32
S33
装置のタイプは
Dev3又はDev4？
Dev3
Dev4
S34
リポケーションリスト/
レジストレーションリスト読出
ID_Bチェック
リポケーションリスト/
レジストレーションリスト送信
S35
リポケーションリスト/
レジストレーションリストの
バージョンは
A＞B又はA＝B又はA＜B？
A>B
A<B
A=B
S36
リポケーションリスト/
レジストレーションリスト読出
$RevV_B$/$RegV_B$チェック
ID_Bチェック
TCsigチェック
リポケーションリスト/
レジストレーションリスト送信
S37
リポケーションリスト/
レジストレーションリスト読出
$RevV_A$/$RegV_A$チェック
ID_Bチェック
TCsigチェック
S38
リポケーションリスト/
レジストレーションリスト受信
$RevV_B$/$RegV_B$チェック
ID_Bチェック
TCsigチェック
リポケーションリスト/
レジストレーションリスト書込
S39
処理は記録又は再生？
記録
再生
S40
Enc(Kse,Kco)受信、復号
Enc(Kst,Kco)計算、書込
Enc(Kco,data)受信、書込
S41
Enc(Kst,Kco)受信、復号
Enc(Kse,Kco)計算、送信
Enc(Kco,data)読出、送信
エンド

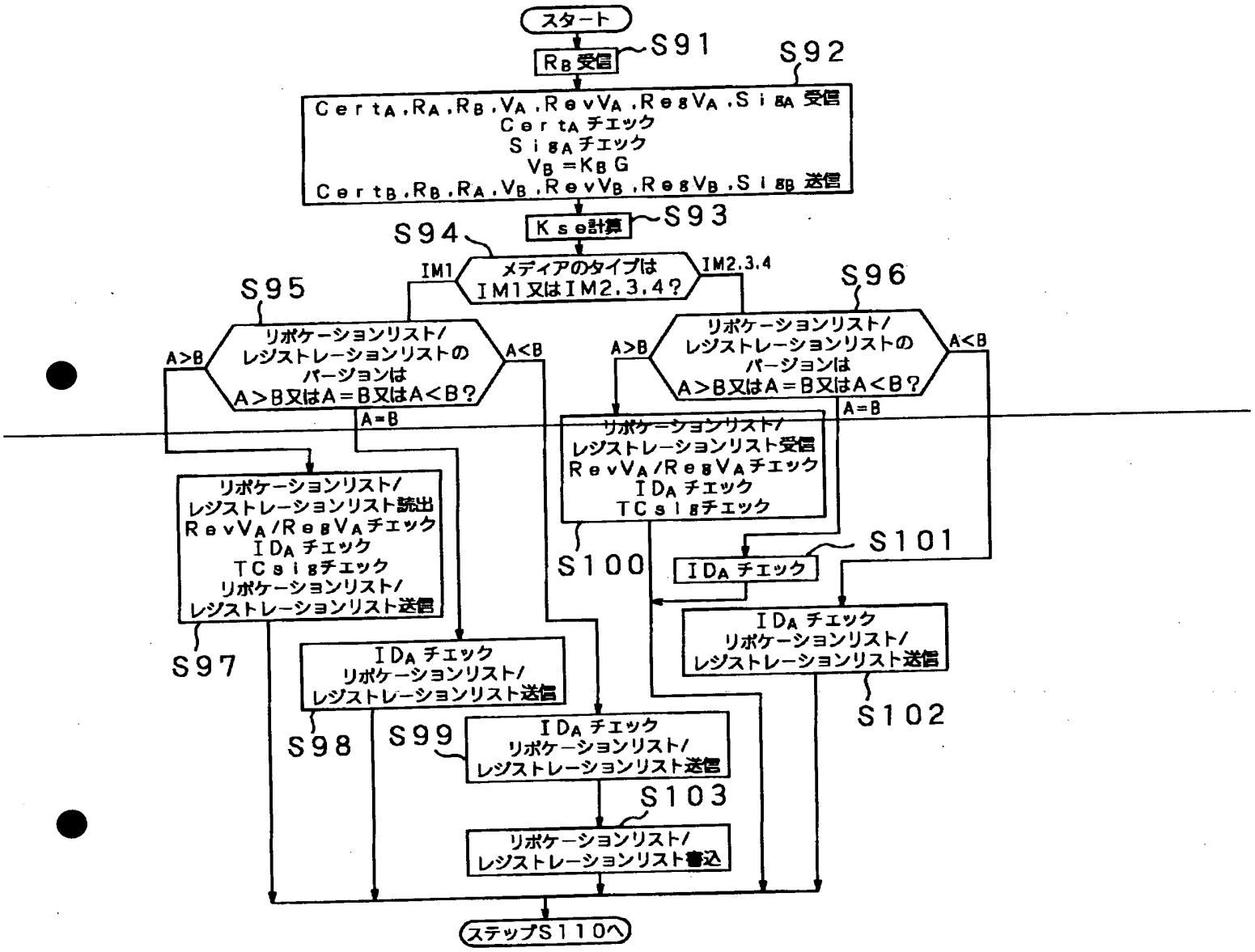
【図８４】


スタート
RB受信
VA＝KA G
RA生成
SigA計算
CertA,RA,RB,VA,RevVA,RegVA,SigA送信
S51
CertB,RB,RA,VB,RevVB,RegVB,SigB受信
CertBチェック
SigBチェック
Kse計算
S52
S53
装置のタイプは
Dev3又はDev4？
Dev3
Dev4
S54
IDBチェック
リポケーションリスト/
レジストレーションリスト送信
S55
リポケーションリスト/
レジストレーションリストの
バージョンは
A＞B又はA＝B又はA＜B？
A>B
A<B
A=B
IDBチェック
S57
S56
IDBチェック
リポケーションリスト/
レジストレーションリスト送信
S58
リポケーションリスト/
レジストレーション受信
RevVB/RegVBチェック
IDBチェック
TCsigチェック
S59
処理は記録又は再生？
記録
再生
S60
Enc(Kse,Kco)受信、復号
Enc(Kst,Kco)計算、書込
Enc(Kco,data)受信、書込
S61
Enc(Kst,Kco)受信、復号
Enc(Kse,Kco)計算、送信
Enc(Kco,data)読出、送信
エンド

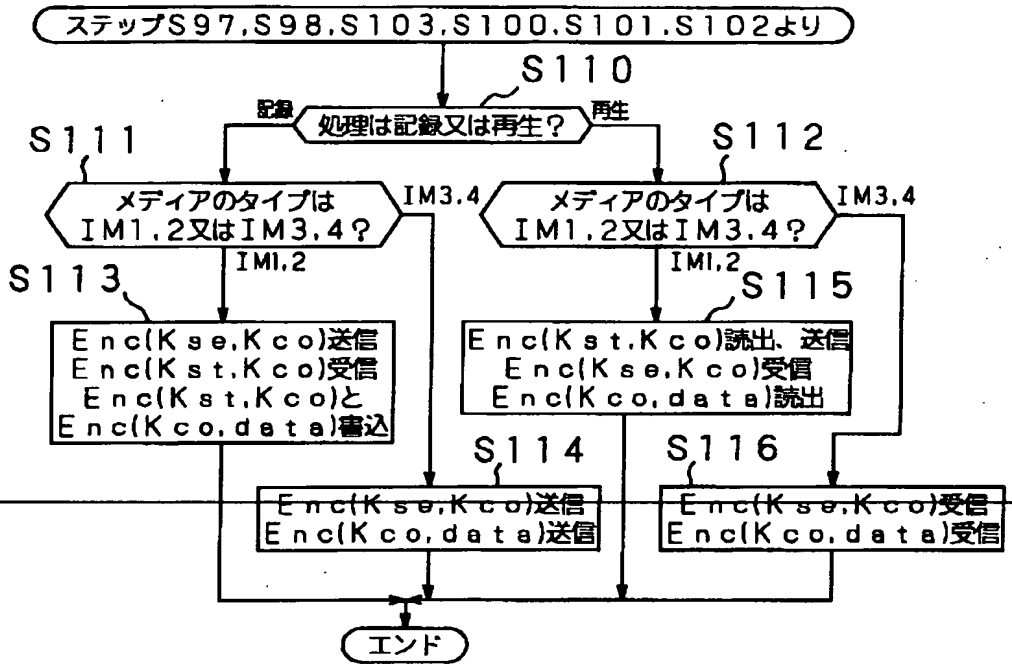
【図８５】


スタート
R_B 送信
S71
$Cert_A, R_A, R_B, V_A, RevV_A, RegV_A, Sig_A$ 受信
$Cert_A$ チエック
Sig_A チエック
$V_B = K_B G$
$Cert_B, R_B, R_A, V_B, RevV_B, RegV_B, Sig_B$ 送信
S72
Kse計算
S73
S74
メディアのタイプは IM1又はIM2,3,4?
IM1
IM2,3,4
S75
S76
リポケーションリスト/ レジストレーションリスト読出
$RevV_A/RegV_A$ チエック
ID_A チエック
TCsigチエック
リポケーションリスト/ レジストレーションリスト送信
リポケーションリスト/ レジストレーションリスト受信
$RevV_A/RegV_A$ チエック
ID_A チエック
TCsigチエック
S77
処理は記録又は再生?
記録
再生
S78
S79
メディアのタイプは IM1,2又はIM3,4?
IM3,4
IM1,2
S80
Enc(Kse,Kco)送信
Enc(Kst,Kco)受信
Enc(Kst,Kco)と Enc(Kco,data)書込
S82
Enc(Kst,Kco)読出、送信
Enc(Kse,Kco)受信
Enc(Kco,data)読出
S81
Enc(Kse,Kco)送信
Enc(Kco,data)送信
S83
Enc(Kse,Kco)受信
Enc(Kco,data)受信
エンド

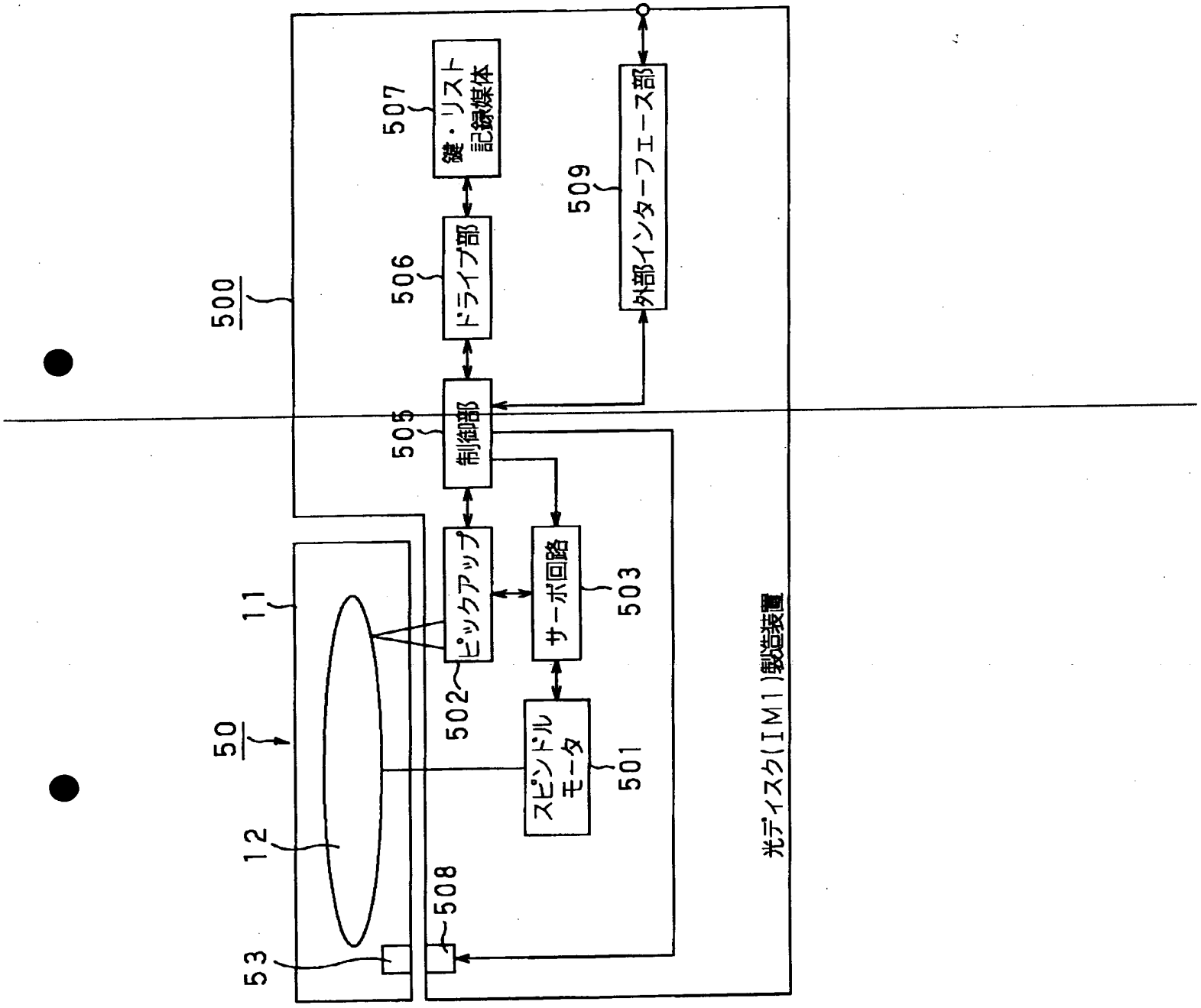
【図８６】


スタート
RB受信
S91
S92
CertA,RA,RB,VA,RevVA,RegVA,SigA 受信
CertA チェック
SigA チェック
VB=KB G
CertB,RB,RA,VB,RevVB,RegVB,SigB 送信
Kse計算
S93
S94
メディアのタイプは
IM1又はIM2,3,4？
IM1
IM2,3,4
S95
S96
リポケーションリスト/
レジストレーションリストの
バージョンは
A>B又はA=B又はA<B？
A>B
A<B
A=B
リポケーションリスト/
レジストレーションリスト読出
RevVA/RegVA チェック
IDA チェック
TCsig チェック
リポケーションリスト/
レジストレーションリスト送信
S97
リポケーションリスト/
レジストレーション受信
RevVA/RegVA チェック
IDA チェック
TCsig チェック
S100
IDA チェック
S101
IDA チェック
リポケーションリスト/
レジストレーションリスト送信
S98
S99
S102
IDA チェック
リポケーションリスト/
レジストレーションリスト送信
S103
リポケーションリスト/
レジストレーションリスト書込
ステップS110へ

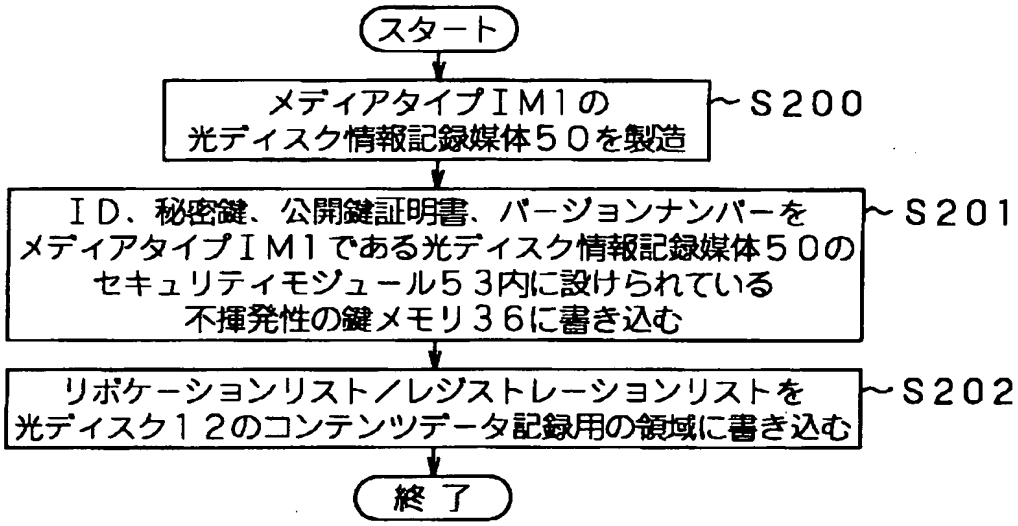
【図８７】


ステップS97,S98,S103,S100,S101,S102より
S110
処理は記録又は再生？
記録
再生
S111
メディアのタイプは
IM1,2又はIM3,4？
IM3,4
IM1,2
S112
メディアのタイプは
IM1,2又はIM3,4？
IM3,4
IM1,2
S113
Enc(Kse,Kco)送信
Enc(Kst,Kco)受信
Enc(Kst,Kco)と
Enc(Kco,data)書込
S115
Enc(Kst,Kco)読出、送信
Enc(Kse,Kco)受信
Enc(Kco,data)読出
S114
Enc(Kse,Kco)送信
Enc(Kco,data)送信
S116
Enc(Kse,Kco)受信
Enc(Kco,data)受信
エンド

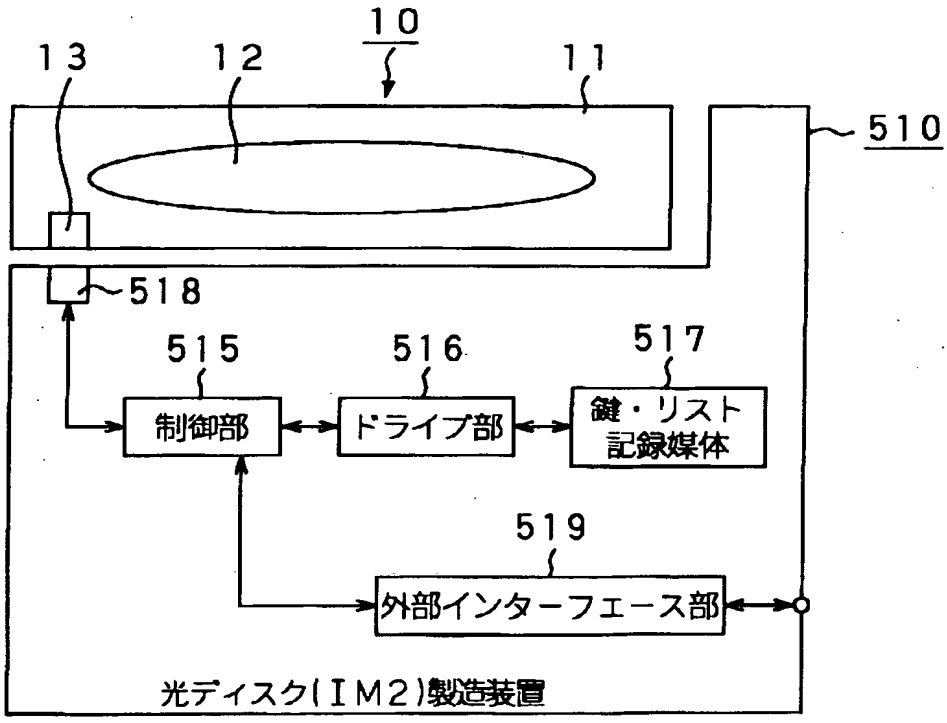
【図８８】


500
507
鍵・リスト記録媒体
506
ドライブ部
509
外部インターフェース部
505
制御部
ピックアップ
サーボ回路
503
502
スピンドルモータ
501
50
11
12
53
508
光ディスク(IM1)製造装置

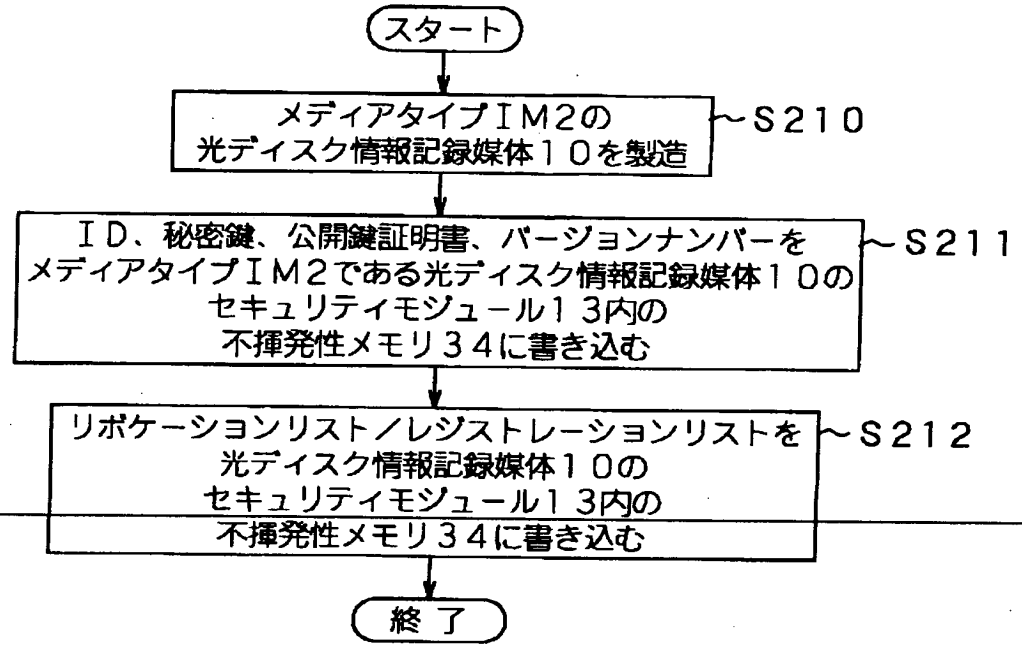
【図８９】


スタート
メディアタイプＩＭ１の
光ディスク情報記録媒体５０を製造
～Ｓ２００
ＩＤ、秘密鍵、公開鍵証明書、バージョンナンバーを
メディアタイプＩＭ１である光ディスク情報記録媒体５０の
セキュリティモジュール５３内に設けられている
不揮発性の鍵メモリ３６に書き込む
～Ｓ２０１
リボケーションリスト／レジストレーションリストを
光ディスク１２のコンテンツデータ記録用の領域に書き込む
～Ｓ２０２
終了

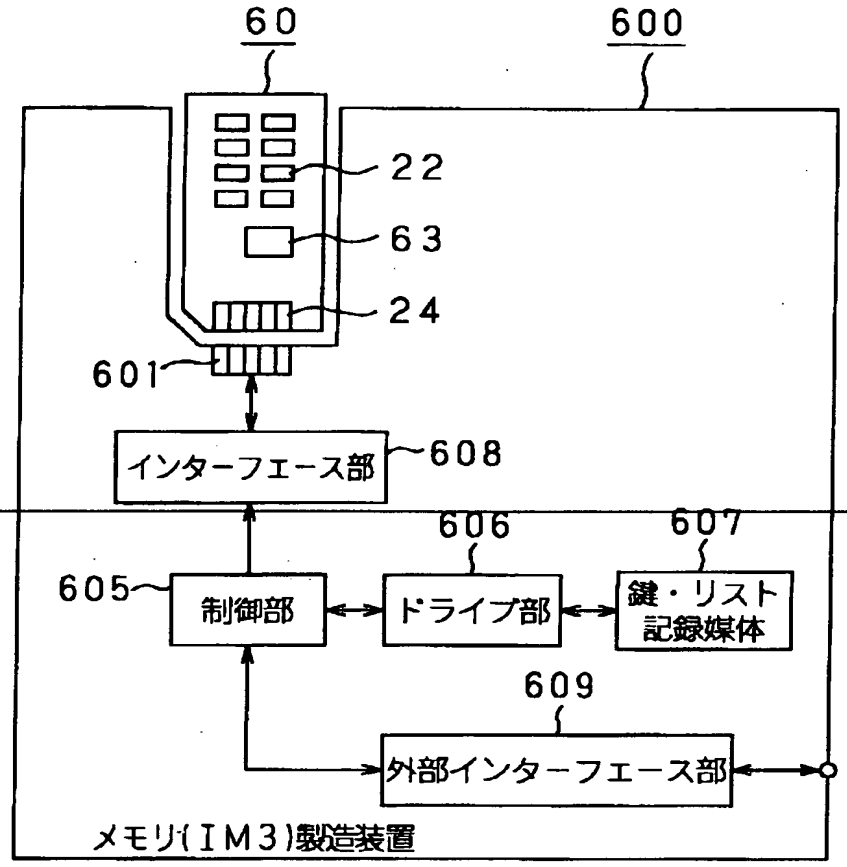
【図９０】


10
13
12
11
510
518
515
516
517
制御部
ドライブ部
鍵・リスト
記録媒体
519
外部インターフェース部
光ディスク(ＩＭ２)製造装置

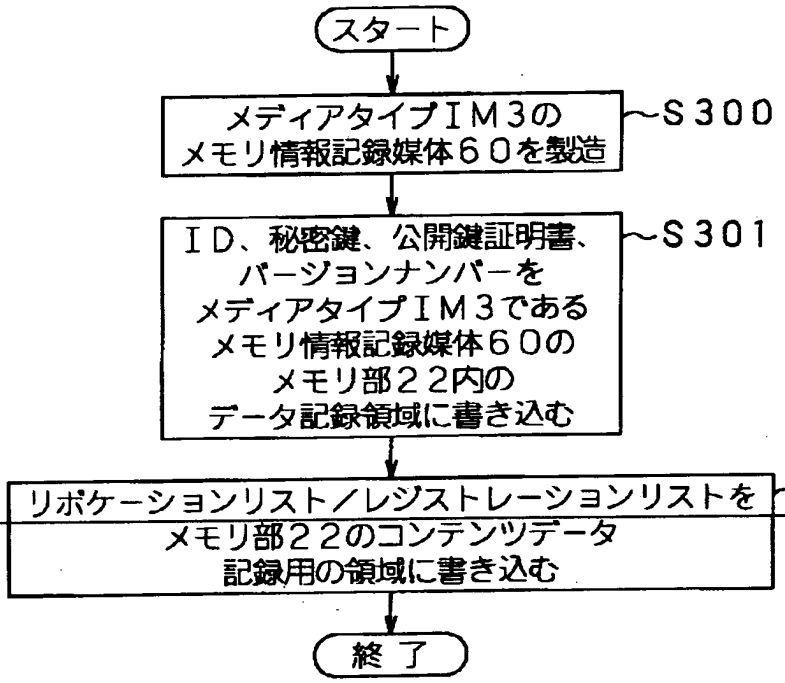
【図９１】


スタート
メディアタイプＩＭ2の
光ディスク情報記録媒体１０を製造
～S210
ＩＤ、秘密鍵、公開鍵証明書、バージョンナンバーを
メディアタイプＩＭ２である光ディスク情報記録媒体１０の
セキュリティモジュール１３内の
不揮発性メモリ３４に書き込む
～S211
リボケーションリスト／レジストレーションリストを
光ディスク情報記録媒体１０の
セキュリティモジュール１３内の
不揮発性メモリ３４に書き込む
～S212
終了

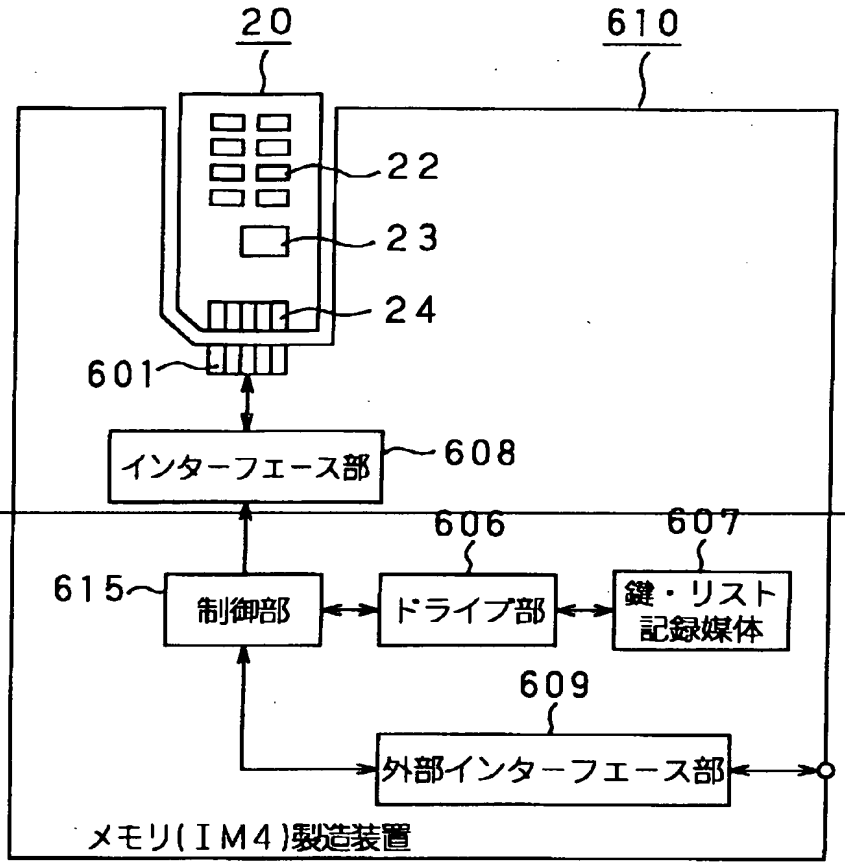
【図９２】


60
600
22
63
24
601
インターフェース部
608
606
607
605
制御部
ドライブ部
鍵・リスト
記録媒体
609
外部インターフェース部
メモリ(IM3)製造装置

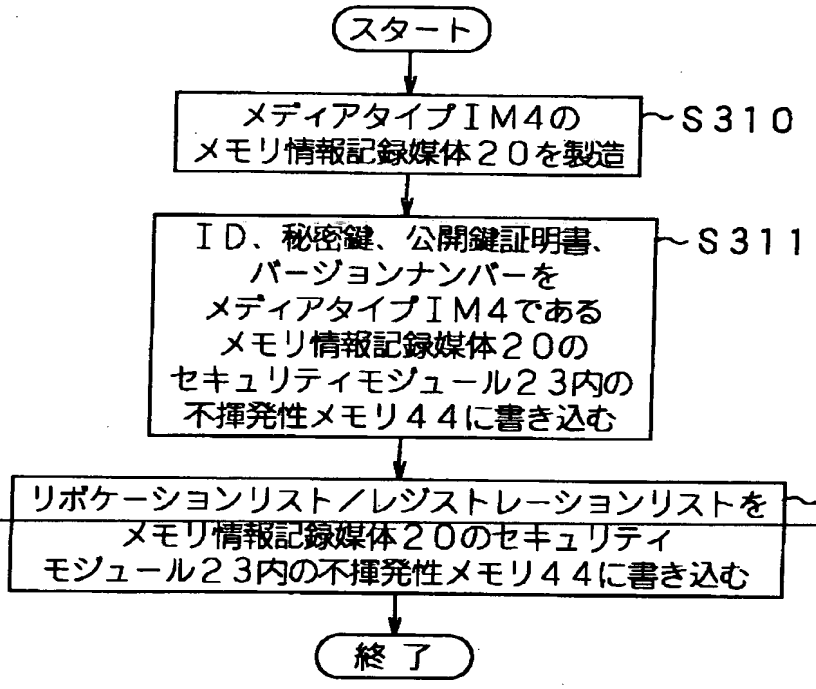
【図９３】


スタート
メディアタイプＩＭ３の
メモリ情報記録媒体６０を製造
S300
ＩＤ、秘密鍵、公開鍵証明書、
バージョンナンバーを
メディアタイプＩＭ３である
メモリ情報記録媒体６０の
メモリ部２２内の
データ記録領域に書き込む
S301
リポケーションリスト／レジストレーションリストを
メモリ部２２のコンテンツデータ
記録用の領域に書き込む
S302
終了

【図９４】


20
610
22
23
24
601
インターフェース部
608
606
607
615
制御部
ドライブ部
鍵・リスト
記録媒体
609
外部インターフェース部
メモリ(ＩＭ４)製造装置

【図９５】


スタート
メディアタイプＩＭ４の
メモリ情報記録媒体２０を製造
S３１０
ＩＤ、秘密鍵、公開鍵証明書、
バージョンナンバーを
メディアタイプＩＭ４である
メモリ情報記録媒体２０の
セキュリティモジュール２３内の
不揮発性メモリ４４に書き込む
S３１１
リボケーションリスト／レジストレーションリストを
メモリ情報記録媒体２０のセキュリティ
モジュール２３内の不揮発性メモリ４４に書き込む
S３１２
終了

【書類名】　　要約書

【要約】

【課題】　映画や音楽などの著作権があるデータの不正な（著作権者の意に反する）複製を防ぐことができるようにする。

【解決手段】　光ディスク情報記録媒体１０にセキュリティモジュール１３を持たせ、光ディスク上に記録されるデータを個々のデータ毎に異なる暗号鍵で暗号化し、暗号鍵をセキュリティモジュール１３が安全に保管する。また、セキュリティモジュール１３は、記録再生装置と公開鍵暗号技術を用いた相互認証を行い、相手が正当なライセンスを受けた装置であることを確認した上で、暗号鍵を装置に対して与えることにより、不正な装置にはデータを漏らさないようにする。

【選択図】　図１

認定・付加情報

特許出願の番号	平成１１年　特許願　第３６３２６６号
受付番号	５９９０１２４７９６４
書類名	特許願
担当官	第八担当上席　　００９７
作成日	平成１２年　１月　６日

＜認定情報・付加情報＞

【特許出願人】

【識別番号】	000002185
【住所又は居所】	東京都品川区北品川６丁目７番３５号
【氏名又は名称】	ソニー株式会社

【代理人】　申請人

【識別番号】	100067736
【住所又は居所】	東京都港区虎ノ門２－６－４　第１１森ビル　小池国際特許事務所
【氏名又は名称】	小池　晃

【選任した代理人】

【識別番号】	100086335
【住所又は居所】	東京都港区虎ノ門２丁目６番４号　第１１森ビル　小池国際特許事務所
【氏名又は名称】	田村　榮一

【選任した代理人】

【識別番号】	100096677
【住所又は居所】	東京都港区虎ノ門二丁目６番４号　第１１森ビル　小池国際特許事務所
【氏名又は名称】	伊賀　誠司

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　　東京都品川区北品川６丁目７番３５号
氏　名　　ソニー株式会社